Reglas y Procedimientos de Seguridad

31 March 2016

SP

Resumen de Cambios, 31 de marzo de 2016

Este manual refleja los cambios relacionados con los anuncios publicados en los boletines de MasterCard del 13 de marzo de 2015 al 1 de marzo de 2016 y los cambios adicionales a la terminología.

Los cambios a este manual no se pueden localizar en línea usando la casilla Find [Buscar]. Haga clic en los números de la sección del enlace para localizar los cambios que se indican a continuación.

Descripción del Cambio	Dónde Buscar
Definiciones actualizadas de los siguientes términos: Método de Verificación del Tarjetahabiente (CVM); Transacción Internacional; Transacción Entre Regiones; Transacción Dentro de la Región; Transacción Dentro de la Región; Cuenta de MasterCard; MasterCard Europe; Verificación del Tarjetahabiente en el Dispositivo; Aplicación de Pago; Terminal del Punto de Venta (POS); Transacción.	Apéndice D (Se reordenó)
Se agregaron las definiciones de los siguientes términos: Sistema de Activación de Cuentas; BIN; Método de Verificación del Tarjetahabiente del Dispositivo del Consumidor, CVM del Dispositivo del Consumidor, CDCVM; Transacción Entre Países de Europa; Transacción Dentro de Europa; Transacción Dentro de Europa que No son SEPA; Caja Fuerte de Token de MasterCard; Sistema de Manejo de las Transacciones; Gerente de Servicios Confiables.	Apéndice D (Se reordenó)
Se agregó la Región de Asia/Pacífico y la Región de Medio Oriente/Africa al alcance de los requisitos para las Aplicaciones de Pago que residen en el Chipe de una Tarjeta.	3.1
Se actualizó la referencia de MasterCard Europe SPRL a MasterCard Europe SA.	3.1
Se agregó 222100 a 272099 al rango del BIN para los PAN de la Cuenta de MasterCard.	3.2
Se eliminaron los requisitos IIN para las Cuentas de Maestro y las Cuentas de Cirrus.	3.3
Se actualizaron los requisitos de la asignación del BIN de la ISO para los emisores de las Tarjetas Maestro y de las Tarjetas Cirrus.	3.3
Se actualizaron los requisitos de apoyo de autorización fuera de línea para las Tarjetas con Chip.	3.6
Se agregó la sección 3.9—Métodos de Verificación del Tarjetahabiente del Dispositivo del Consumidor	3.9

Descripción del Cambio	Dónde Buscar
Se agregó la sección 3.9.1—Calificación de MasterCard de los CVM del Dispositivo del Consumidor	3.9.1
Se agregó la sección 3.9.2—Funcionalidad por CDCVM.	3.9.2
Se agregó la sección 3.9.3—Autenticación Persistente.	3.9.3
Se agregó la sección 3.9.4—Autenticación Prolongada.	3.9.4
Se agregó la sección 3.9.5—Cómo Mantener el Estado del CVM Calificado por MasterCard.	3.9.5
Se agregó la sección 3.9.6—Responsabilidades del Emisor.	3.9.6
Se aclararon los requisitos del límite de parámetros para la autenticación prolongada del Tarjetahabiente.	3.9.6
Se agregó la sección 3.9.7—Uso de un Proveedor.	3.9.7
Se eliminó la sección 3.11—Documentos de Información de la Transacción (TID)	3.11 (se eliminó)
Se eliminó la sección 3.11.1—Contenido de los Juegos de Formularios.	3.11.1 (se eliminó)
Se eliminó la sección 3.11.2—Contenido de los Recibos de Terminales de POS.	3.11.2 (se eliminó)
Se eliminó la sección 3.11.3—Truncamiento del Número de Cuenta Primario y Omisión de la Fecha de Vencimiento.	3.11.3 (se eliminó)
Se aclararon los requisitos del indicador de rendimiento relacionados con la herramienta de detección de fraude del Emisor.	6.2.1.7
Se aclararon los requisitos de acatamiento del MATCH para los Adquirientes.	7.1.2
Se actualizaron las referencias de los Comercios/Comercios Secundarios/ Transacciones de lotería estatal a Comercios/Comercios Secundarios/ Transacciones de lotería gubernamental para los tipos de entidades que deben cumplir con la inscripción y los requisitos de control del MRP.	7.4 9.1 9.3
Se agregaron los Comercios y Comercios Secundarios de cyberlocker de alto riesgo de los tipos de entidades que deben cumplir con los requisitos de inscripción y control del MRP.	7.4 9.1 9.2.1 9.3
Se eliminó la sección 8.1—Cómo Presentar Transacciones Válidas	8.1 (se eliminó)
Se agregó la sección 8.1—Cómo Notificar a MasterCard	8.1
Se eliminó la sección 8.1.1—Cómo Notificar a MasterCard—Responsabilidades del Adquiriente	8.1.1 (se eliminó)

Descripción del Cambio	Dónde Buscar
Se agregó la sección 8.1.1—Responsabilidades del Adquiriente	8.1.1
Se eliminó la sección 8.1.2—Cómo Notificar a MasterCard—Responsabilidades del Emisor	8.1.2 (se eliminó)
Se agregó la sección 8.1.2—Responsabilidades del Emisor.	8.1.2
Se eliminó la sección 8.1.3—Auditoría de MasterCard.	8.1.3 (se eliminó)
Se eliminó la sección 8.1.3.1—Inicio de la Auditoría de MasterCard	8.1.3.1 (se eliminó)
Se eliminó la sección 8.1.3.2—Información Requerida por MasterCard	8.1.3.2 (se eliminó)
Se eliminó la sección 8.1.3.3—Notificación a los Clientes del Período de Contracargos	8.1.3.3 (se eliminó)
Se actualizó la referencia cruzada a la Regla de Transacciones Válidas del manual *Reglamento de MasterCard*.	8.2.1
Se actualizó el cargo anual de uso del MATCH a US$5.000.	8.2.6.1 11.2
Se movieron los contenidos de la sección 8.4.3—Notificación de MasterCard a los Emisores a la sección 8.4.3.1—Investigaciones que Involucran Cuentas "Bust-out" del Tarjetahabiente (nueva).	8.4.3.1
Se agregaron nuevos contenidos a la sección 8.4.3—Notificación de MasterCard a los Emisores.	8.4.3
Se agregó la sección 8.4.3.2—Investigaciones que No Involucran Cuentas "Bust-out" del Tarjetahabiente.	8.4.3.2
Se agregó el MCC 9406 a los tipos de Comercios de lotería gubernamental, requerido para estar inscrito usando el MRP.	9.1
Se agregó la sección 9.4.6—Comercios de Cyberlocker de Alto Riesgo.	9.4.6
Se movió la sección 9.4.4—Comercios de Lotería Estatal (Región de EE. UU. Solamente) a la sección 9.4.4.1.	9.4.4.1
Se agregó la sección 9.4.4—Comercios de Lotería propiedad del Gobierno.	9.4.4
Se agregó la sección 9.4.4.2—Comercios de Lotería propiedad del Goberino (Países Específicos).	9.4.4.2
Se aclaró el propósito y la ubicación de las Normas de Seguridad de la PCI.	10.1
Se aclaró el alcance de la lista de la terminología del Evento de Compromiso de los Datos de la Cuenta.	10.2
Se aclararon los criterios de conocimiento del Evento de ADC/Evento Potencial de ADC para los Clientes y los Agentes de Clientes.	10.2.2.1

Descripción del Cambio	Dónde Buscar
Se agregaron referencias a otros Agentes a las referencias aplicables de los Comercios.	10.2.2.1 10.2.4 10.2.5.3
Se aclararon los contenidos requeridos del informe forense final.	10.2.3
Se actualizó el número de Cuentas a 30.000 para el Criterio A.	10.2.4
Se actualizaron los requisitos del Cliente responsable para el Criterio C.	10.2.4
Se actualizó la referencia del Contacto del Adquiriente del Comercio al Contacto de Compromiso de los Datos de la Cuenta.	10.2.5.2
Se actualizaron los criterios de participación del Emisor para el componente de reembolso del Programa de ADC.	10.2.5.3
Se actualizaron los requisitos de responsabilidad financiera del Cliente responsable en relación al Evento de ADC.	10.2.5.3
Se actualizó el proceso de determinación de la OR del ADC.	10.2.5.4
Se actualizaron las referencias de las Terminales Híbridas del POS de la Interfaz Dual a Terminales Híbridas del POS.	10.2.5.4 10.2.5.5 10.3.4.2
Se actualizó el proceso de determinación de la FR del ADC.	10.2.5.5
Se actualizaron los requisitos de presentación de informes al SAFE para los Emisores con respecto a las Cuentas que se encuentran en riesgo de un Evento de ADC o de un Evento Potencial de ADC.	10.2.5.5
Se agregó el encabezador de la sección Deducción en el Contracargo.	10.2.5.5
Se agregó la sección Impacto del Cambio de Responsabilidad del Chip.	10.2.5.5
Se aclararon los criterios de elegibilidad de recuperación de fraude de ADC para las Cuentas divulgadas por Eventos de ADC diferentes.	10.2.5.5
Se eliminó la sección 10.2.5.6—Investigación y Otros Costos.	10.2.5.6 (se eliminó)
Se actualizó el proceso de determinación final de la responsabilidad financiera.	10.2.7
Se aclaró la descripción del código de motivo 04 del MATCH.	Tabla 11.4
Se aclararon los requisitos de presentación de informes al SAFE para los Emisores.	12.1
Se actualizaron los requisitos de presentación de informes al SAFE para las Transacciones de Pago a Distancia Digital Garantizado.	12.2.1

Descripción del Cambio	Dónde Buscar
Se eliminó el Apéndice B—Especificaciones de los Juegos de Formularios.	Apéndice B (se eliminó)
Se eliminó el Apéndice D—Guías de Mejores Prácticas.	Apéndice D (se eliminó)

Contenido

Capítulo 1 Obligaciones del Cliente

Este capítulo describe las obligaciones generales del Programa y de acatamiento del Cliente relacionadas con la emisión de Tarjetas de MasterCard y las Actividades del Programa de adquisición del Comercio.

1.1 Acatamiento de las Normas

Este manual contiene Normas. Cada Cliente debe acatar por completo estas Normas.

Todas las Normas en este manual se asignan a la categoría de no acatamiento A en la estructura de acatamiento descrita en el Capítulo 2 del manual *Reglamento de MasterCard* ("la estructura de acatamiento"), a menos que se especifique de otro modo en la tabla a continuación. El programa de recargos por no acatamiento proporcionado en la estructura de acatamiento aplica a cualquier Norma en el manual *Security Rules and Procedures* que no tenga un Programa de acatamiento establecido. La Corporación puede desviarse del programa en cualquier momento.

Número de Sección	Título de la Sección	Categoría
1.3	El Contacto de Seguridad	C
2.3	Contratación con Compañías de Registro de Tarjetas	C
7.1.5	Retención de los Registros de Investigación	C

1.2 Conflictos Legales

Un cliente está exento de acatar una Norma en cualquier país o región de un país solamente hasta el punto en que tal acatamiento podría provocar que el Cliente viole la ley local o regulación aplicable y, siempre y cuando que el Cliente avise rápidamente a la Corporación, por escrito, la base y el origen de tal incapacidad de acatamiento. La Corporación tiene la autoridad de aprobar alternativas locales a estas Normas.

1.3 El Contacto de Seguridad

Cada Cliente debe tener un Contacto de Seguridad listado para cada uno de sus números de Identificación del Miembro/ICA en la herramienta de Información del Miembro en MasterCard Connect™.

Capítulo 2 Normas de Producción de Tarjetas

Este capítulo puede ser de interés especial para los Clientes que emiten Tarjetas, e incluye los requisitos para el personal a cargo de las tareas relacionadas con la producción de Tarjetas.

2.1 Acatamiento de las Normas de Producción de Tarjetas

Según se utiliza en esta sección, y excepto que se especifique otra cosa, el término "Producción de tarjetas" se aplica con relación a las Tarjetas y a otro tipo de Dispositivos de Acceso, que incluyen los Dispositivos de Pago Móviles y los Dispositivos de Pago Sin Contacto.

Un Emisor que participa en la producción de Tarjetas debe acatar todas las Normas correspondientes, incluyendo, entre otras, las estipuladas en este capítulo y en los siguientes documentos:

- *Normas de Diseño de Tarjetas*
- *Card Production Physical Security Requirements [Requisitos de Seguridad Física de la Producción de Tarjetas]*
- *Card Production Logical Security Requirements [Requisitos de Seguridad Lógica de la Producción de Tarjetas]*
- *Security Requirements for Mobile Payment Provisioning [Requisitos de Seguridad para la Provisión de Pago Móvil]*

Los documentos *Card Production Physical Security Requirements [Requisitos de Seguridad Física de la Producción de Tarjetas]* y *Card Production Logical Security Requirements [Requisitos de Seguridad Lógica de la Producción de Tarjetas]* están disponibles en el sitio web del Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (SSC de la PCI) bajo la pestaña **Card Production [Producción de Tarjetas]** en www.pcisecuritystandards.org/security_standards/documents.php.

Un Emisor que utiliza un proveedor de producción de Tarjetas para producir Tarjetas en su nombre debe acatar también las Normas establecidas en la sección 2.4 de este manual.

Se recomienda que los Emisores que emiten y/o personalizan Tarjetas en el sitio en una sucursal bancaria, tienda minorista u otra ubicación fuera de las instalaciones del proveedor de producción de Tarjetas consulten el manual *Security Guidelines for Instant Card Issuance and Instant Card Personalization* para obtener información acerca de la emisión segura de Tarjetas y de la protección de los datos del Tarjetahabiente en dichas ubicaciones.

Las actividades de producción de tarjetas sujetas al acatamiento de estas Normas incluyen, a título ilustrativo y no limitativo, el trato y la protección de las Tarjetas, la fabricación de las Tarjetas, la impresión, el grabado en relieve, la codificación y el envío por correo de las tarjetas, así como cualquier etapa de la producción y distribución de las Tarjetas o la información de la cuenta de la Tarjeta.

Consulte el Apéndice C de este manual para obtener descripciones detalladas de las actividades de producción de Tarjetas.

2.2 Cómo Controlar el Personal

Siempre que lo permita la ley, los Emisores deberán llevar a cabo investigaciones de crédito y antecedentes penales de todo el personal que maneje Tarjetas con grabado en relieve o sin grabado en relieve, incluyendo empleados de tiempo parcial y temporales.

Además, siempre que lo permita la ley, los Emisores no deberán emplear personal con una o más condenas penales, con antecedentes de crédito de alto riesgo o ambos, en las áreas donde se almacenen o se procesan Tarjetas.

Los emisores no deberán tampoco permitir el acceso a estos empleados a los números de cuenta, Tarjetas con grabado en relieve o sin grabado en relieve, equipo grabado en relieve o codificado, ni deberán emplearlos en trabajos relacionados con la seguridad o el procesamiento de desperdicios.

2.3 Cómo Contratar Compañías de Registro de Tarjetas

Una compañía de registro de tarjetas ("Compañía") es cualquier entidad que almacena números de cuenta de Tarjetas y que, tras la notificación del Tarjetahabiente, informa el extravío o robo de las Tarjetas a los Emisores.

Cualquier Emisor que tenga un convenio contractual con una Compañía según el cual la Compañía registra los números de cuenta del Tarjetahabiente del Emisor, deberá cerciorarse de que el contrato incluya las siguientes obligaciones por parte de la Compañía:

- La Compañía deberá mantener cualquier información del Tarjetahabiente estrictamente confidencial incluyendo entre otros, los nombres, las direcciones, los teléfonos y los números de cuenta que los revelará solamente al Emisor. La Compañía deberá guardar cualquier medio que contenga este tipo de información en un área limitada al personal seleccionado que tenga acceso sobre la base de su necesidad a esta información. Antes de desechar cualquiera de estos medios, la Compañía deberá destruirlo de manera que los datos queden ilegibles.
- La Compañía controlará y limitará el acceso a los números de cuenta almacenados en un entorno de computadoras, estableciendo procedimientos que deben incluir, entre otros, un sistema de contraseñas de acceso remoto a la terminal (CRT) por computador y control de las líneas de marcado o cualquier otro medio de acceso.
- La Compañía no podrá utilizar el nombre de MasterCard en ninguna promoción ni publicidad, excepto cuando esté previsto mediante un convenio contractual con el Emisor para fines de ofrecer y prestar servicios a los Tarjetahabientes del Emisor. MasterCard se reserva el derecho de aprobar dichos materiales.
- La Compañía deberá mantener un servicio que funcione 24 horas al día, los siete días de la semana para recibir los informes de los Tarjetahabientes sobre Tarjetas robadas o extraviadas. La Compañía transmitirá cada informe inmediatamente y en todo caso a más tardar dos horas después de recibir el informe y por los medios más rápidos disponibles, por ejemplo, teléfono o fax, al Emisor apropiado.

Como mínimo, la notificación deberá incluir:

  - Número de cuenta
  - Nombre del emisor
  - Nombre, dirección y número de teléfono del tarjetahabiente
  - Número de teléfono donde se puede encontrar al Tarjetahabiente
  - Si la Tarjeta fue robada o extraviada
  - Hora y lugar de la pérdida o robo informado
- La Compañía deberá reportar cualquier pérdida o robo de información del Tarjetahabiente, debida a acto u omisión, a MasterCard y al Emisor con el cual tenga un contrato, dentro de un plazo de 24 horas del descubrimiento de la pérdida o robo.
- La Compañía debe hacer llegar una solicitud de Tarjeta de reposición del Tarjetahabiente al Emisor.
- El contrato deberá incluir una cláusula de indemnización que ampare a MasterCard, sus funcionarios, directores y empleados, sus Clientes y al Emisor que tenga el contrato con la Compañía de toda pérdida o daño por cualquier reclamo que presente o se presente a nombre del Tarjetahabiente, Emisor o cualquier otra persona o entidad, la que se supone puede atribuirse a una falla de la Compañía en prestar adecuadamente los servicios descritos en el contrato o a una falla en la protección de la información de la cuenta.
- La Compañía deberá contar con cobertura de seguro contra responsabilidad civil, seguro de fidelidad, seguro contra incendio y robo y deberá contar, además, con un plan de recuperación por desastres para garantizar la continuidad de los servicios en caso de eventos naturales o de otros eventos que interrumpan o puedan interrumpir el servicio, a menos que MasterCard acuerde lo contrario por escrito. La cobertura deberá ser razonable y adecuada considerando la naturaleza y el volumen del trabajo realizado, la ubicación de la planta, el estado físico y la seguridad de la planta, y el número de empleados y sus responsabilidades.
- La Compañía deberá acatar todas las leyes, reglamentos y regulaciones correspondientes, incluyendo, sin limitación, las leyes que garantizan la protección del consumidor aplicables a los servicios que ofrezca y preste la Compañía.

2.4 Cómo Trabajar con Proveedores

Antes de contratar los servicios de un proveedor para efectuar cualquiera de los servicios de producción de Tarjetas descritos en el Apéndice E de este manual, el Cliente debe asegurarse de que el proveedor haya sido certificado por MasterCard bajo el Programa Global de Certificación de Proveedores (GVCP).

Antes de la certificación y la recertificación anual de las instalaciones de un proveedor bajo el GVCP, MasterCard efectúa una auditoría en las instalaciones para evaluar su acatamiento con las Normas de seguridad físicas, lógicas y de provisión de pago móvil correspondientes establecidas en los siguientes documentos:

- *Card Production Physical Security Requirements [Requisitos de Seguridad Física de la Producción de Tarjetas]*

- *Card Production Logical Security Requirements [Requisitos de Seguridad Lógica de la Producción de Tarjetas]*
- *Security Requirements for Mobile Payment Provisioning [Requisitos de Seguridad para la Provisión de Pago Móvil]*

Los documentos *Card Production Physical Security Requirements [Requisitos de Seguridad Física de la Producción de Tarjetas]* y *Card Production Logical Security Requirements [Requisitos de Seguridad Lógica de la Producción de Tarjetas]* están disponibles en el sitio web del SSC de la PCI bajo la pestaña **Card Production [Producción de Tarjetas]** en www.pcisecuritystandards.org/security_standards/documents.php.

Se expide una certificación de acatamiento a las instalaciones del proveedor certificado. Esta certificación está sujeta a renovación anual siempre que las instalaciones del proveedor permanezcan en acatamiento. La "Lista de Proveedores Certificados", según se publica mensualmente en el *Boletín de Seguridad Global*, contiene el nombre de cada instalación de proveedor certificada y una descripción de los servicios específicos que la instalación está autorizada a efectuar.

Cualquier convenio entre un Emisor y un proveedor para un servicio de producción de Tarjetas debe contener términos que establezcan que el proveedor acepta salvaguardar y controlar el uso de los datos de la cuenta y acatar todas las Normas vigentes correspondientes, incluyendo, entre otras, las Normas establecidas en la sección 2.4 y en el manual *Card Design Standards*.

Para obtener más información sobre el GVCP, comuníquese con MasterCard enviando un correo electrónico a gvcp-helpdesk@mastercard.com.

2.4.1 Order Request Required to Produce Cards

No vendor may print or manufacture any Card, sample, or facsimile, on plastic or any other material, except in response to a specific order from a Customer or from MasterCard. A Customer may order Cards by using the Card Order Request (Form 488), available in the Library section of MasterCard Connect™, or an equivalent document that provides the same information.

Form 488 (or an equivalent document) must be completed and retained by the vendor and Customer, and must be made available to MasterCard upon request.

MasterCard reserves the right to request, from time to time, Card samples for review, and will communicate any such request via the **Submit a Card Design Request (Manufacturer)** process on MasterCard Connect™.

2.4.2 Acumulación de Cantidades de Plástico

El Emisor no podrá alentar a un proveedor a acumular grandes cantidades de plástico o Tarjetas ni usar un proveedor conocido para participar en la práctica de acumular grandes cantidades de plástico o Tarjetas. La acumulación de grandes cantidades es la práctica de fabricar plásticos o Tarjetas en exceso con anticipación a futuros pedidos de los Clientes.

2.5 Tarjetas Sin Personalización

El Cliente no debe enviar por correo electrónico Tarjetas "incompletas" (según se utiliza el término en el presente documento, "incompletas" se refiere a una Tarjeta que aún no ha sido personalizada con un número de cuenta primario [PAN] o fecha de vencimiento). Las Tarjetas Incompletas se deben enviar mediante métodos de envío seguros según se describe en *Card Production Physical Security Requirements [Requisitos de Seguridad Física de la Producción de Tarjetas]*. En el caso excepcional de que se requiera una entrega rápida y no fuera posible utilizar un método de envío seguro, el Emisor podrá usar un servicio de mensajería rápida que proporcione rastreo del envío, autenticación de quien recibe y confirmación de recepción para el envío de no más de 500 Tarjetas incompletas por día.

2.6 Discrepancias en el Conteo de Tarjetas

Tras recibir un envío de Tarjetas, el Emisor deberá verificar que se entregó la cantidad de Tarjetas correcta y deberá tomar medidas inmediatas para solucionar cualquier discrepancia en el conteo de las Tarjetas y recuperar cualquier Tarjeta faltante. El Emisor puede usar el conteo de Tarjetas que figura en cada cartón sellado para la verificación del conteo de Tarjetas. Los cartones sellados podrán abrirse al azar, auditarse y volver a sellarse. Se debe contar el contenido de todos los cartones abiertos y todos los cartones sellados sin conteo de Tarjetas anotado en el cartón.

2.7 Reporting Card Loss or Theft

Within 24 hours of discovery, a Customer must report to MasterCard the suspected or confirmed loss or theft of any Cards while in transit from a vendor or in the Customer's possession. The report must be sent via email to gvcp-helpdesk@mastercard.com and contain the following information:

- Issuer name and Member ID/ICA number
- Card type and quantity
- With respect to the loss or theft of Cards while in transit from a vendor:
  - The vendor name
  - The location from which the Cards were shipped
  - The date and method of shipment
  - The address to which the Cards were shipped
- Pertinent details about the loss and the investigation
- Name and phone number of contact for additional information
- Name and phone number of person reporting the loss or theft

2.8 Cómo Disponer de las Tarjetas Sin Emitir y de la Información de la Cuenta

Un Cliente que deja de emitir Tarjetas deberá destruir rápidamente o desechar de otra manera adecuada todas las Tarjetas sin emitir y todos los medios que contengan información sobre la Cuenta de Tarjeta.

Capítulo 3 Normas de Diseño del Dispositivo de Acceso y de la Tarjeta

Este capítulo puede ser de interés particular para los Emisores y Proveedores certificados por MasterCard responsables del diseño, creación y control de las Tarjetas. Proporciona las especificaciones de todos los programas de Tarjetas de MasterCard, Maestro y Cirrus en todo el mundo.

3.1 Principios de Estandarización

Todas las Tarjetas se deben poder usar en todos los dispositivos estándares de lectura de la banda magnética de la Tarjeta y, si hay un chip presente, en todas las terminales híbridas, de modo que sea posible el intercambio electrónico de datos de la Transacción.

Todas las Tarjetas grabadas al relieve se deben poder usar en todas las impresoras estándar—la información grabada al relieve debe producir una impresión clara y acatar todas las Normas de posición y tipo de letra.

Todas las tarjetas que contienen un chip deben acatar el EMV. Dichas Tarjetas se llaman Tarjetas con Chip. Todas las Tarjetas con Chip deben tener una sola aplicación principal definida por MasterCard que reside en el chip y en la banda magnética; la información de la Cuenta que aparece en el frente de la Tarjeta debe ser para la aplicación principal residente en la banda magnética. Ninguna Aplicación de Pago residente en el chip de una Tarjeta emitida en la Región de Asia/Pacífico, en la Región de Medio Oriente/Africa o en la Región de Estados Unidos podrá tener una prioridad de aplicación superior a la aplicación principal de la Tarjeta.

Todas las Aplicaciones de Pago en una Tarjeta con Chip deben tener una fecha de validez (si corresponde) y una fecha de vencimiento dentro de las fechas o en la fecha presente en el frente de la Tarjeta. La fecha de validez que aparece en el frente de la Tarjeta debe ser la misma que la de la aplicación principal en la Tarjeta.

NOTA: Una Terminal Híbrida del Punto de Venta (POS) puede leer Transacciones por banda magnética y con chip y debe acatar las normas de EMV, según se establece en la sección 4.8 de este manual.

NOTA: En 1996, Europay (ahora una subsidiaria propiedad exclusiva de MasterCard y con un nombre nuevo, MasterCard Europe SA), MasterCard y Visa desarrollaron Normas para las Tarjetas de circuito integrado (ICC), terminales y aplicaciones. EMVCo, LLC, establecida en 1999, es la organización que fiscaliza y mantiene las especificaciones de EMV.

Todos los Emisores deben acatar las *Normas de Diseño de Tarjetas*, disponibles en MasterCard Connect™, incluyendo entre otros, los requisitos relacionados con:

- Los materiales, dimensiones y medidas del grabado al relieve de la Tarjeta, la banda magnética, el chip, las Marcas y otras características de las Tarjetas;
- Diseño de tarjeta
- Uso de la activación de la Tarjeta y calcomanías de divulgación de autorización selectiva

3.2 Número de Cuenta de MasterCard

El número de cuenta primario (PAN) de una Cuenta de MasterCard identifica el número de identificación bancaria (BIN) del Emisor, la porción del número de cuenta asignada por el Emisor y el dígito de verificación, según se muestra en la Tabla 3.1. El PAN de una Cuenta de

MasterCard comienza con un BIN en el rango de 222100 a 272099 o de 510000 a 559999. Una Cuenta de MasterCard debe usar un BIN asignado por MasterCard.

Tabla 3.1—Configuración de Ejemplo del Número de Cuenta de MasterCard

Número de Cuenta de MasterCard = 5412 75XX XXXX 9999		
La configuración es como sigue:		
5412 75	XX XXXX 999	9
BIN del Emisor asignado por MasterCard	Porción del número de Cuenta asignada por el Emisor	Dígito de verificación

El dígito de verificación se calcula utilizando la Fórmula Luehn para la Computación del Dígito de Verificación de Módulo 10 (“Doble-Suma-Doble”).

3.3 Números de Cuenta Maestro y Cirrus

El PAN de una Cuenta de Maestro o de Cirrus no debe tener menos de 12 dígitos numéricos y no más de 19 dígitos numéricos de longitud. El PAN incluye el número de identificación del Emisor (IIN o BIN), la porción del número de Cuenta individual asignada por el Emisor y el dígito de verificación que se calcula utilizando la Fórmula Luehn para la Computación del Dígito de Verificación de Módulo 10 (“Doble-Suma-Doble”).

Un Cliente puede solicitar que MasterCard asigne un BIN para las Tarjetas de Maestro y Cirrus. MasterCard no permite que se agregue un programa de Maestro a un BIN que no es asignado por MasterCard o sea verificado como que ha sido asignado al Emisor bajo la ISO 7812.**En caso de cualquier disputa relacionada con las asignaciones de BIN de la ISO, es responsabilidad del Emisor solucionar ese conflicto con la ISO.**

3.4 Signature Panel

Upon issuance or reissuance, an Issuer must include written notice to all Cardholders to sign all Cards immediately when received and before initial use. Only the authorized Cardholder (the person whose name appears on the Card front) may sign the Card back. The name signed by the authorized Cardholder must match the name that appears on the Card front, regardless of the language used by the Cardholder to sign his or her name. The Issuer must state this as a condition of Card use. (The vehicle-assigned MasterCard Corporate Fleet Card is exempt from this requirement.)

3.5 Magnetic Stripe or MasterCard HoloMag Encoding

The specifications for the physical and magnetic characteristics of the magnetic stripe on Cards must comply with ISO 7813 Credit Cards—Magnetic Stripe Encoding for Tracks 1 and 2. Production of Card plastics with low coercivity magnetic tape is prohibited. Alternatively, the Issuer may use MasterCard HoloMag™ in place of the magnetic stripe.

The Issuer of a MasterCard Card must ensure that the encoded magnetic stripe contains Track 1 and Track 2 data, and also includes the information specified in this chapter.

For a Maestro Card or Cirrus Card, only the encoding of Track 2 data is required; the encoding of Track 1 data is optional. If Track 3 is encoded, the encoding must comply with ISO 4909 Bank Cards—Magnetic Stripe Content for Track 3.

An Acquirer must transmit the full unedited magnetic stripe data with each magnetic stripe-based electronically authorized Transaction.

NOTA: The transmission of the entire contents of Track 1 or Track 2 data must be unaltered and unedited, and cannot be truncated.

3.5.1 Código de Validación de la Tarjeta 1 (CVC 1)

La Pista 1 y la Pista 2 de la banda magnética deben estar codificadas con un valor de CVC 1. Consulte la sección 3.10.5 de este manual para conocer los requisitos del código de validación de Tarjetas, los métodos de cálculo y los datos de verificación.

3.5.2 Código de Servicio

La Pista 1 y Pista 2 de la banda magnética deben contener un valor de código de servicio codificado de tres dígitos. Consulte la sección 3.11 de este manual para conocer los requisitos de uso del código de servicio.

3.5.3 Cardholder Name

NOTA: The Cardholder's name must be present in the Account Information Area and encoded on the magnetic stripe.

The encoded Cardholder Name field in Track 1 is a variable length, alphanumeric field, with a maximum length of 26 characters within (up to) three subfields. Due to the variable length of the field, the starting position of each remaining field depends on the ending position of the Cardholder name. The Cardholder Name and Content Format table shown in Appendix A defines the specifications for encoding the Cardholder name on the magnetic stripe.

NOTA: Characters "%", "^", and "?" cannot be used in the Cardholder Name field, because they are used only for specified encoding purposes.

Use the following specifications to encode the Cardholder name on the magnetic stripe of all Cards:

- If the Card is a MasterCard Corporate Card product, the Cardholder name encoded on Track 1 and the name present in the Account Information Area should be the same, although the formats are different.

  For example:

  BROWN/ROBERT S
- Issuers engaged in the instant issuance and/or instant personalization of Cards under the MasterCard Unembossed or MasterCard Electronic Programs or the issuance of non-personalized prepaid Cards must ensure that when a Program name appears on the Card front in place of the Cardholder name, the same Program name is also encoded in the Cardholder Name field in Track 1.
- The magnetic stripe may encode a Cardholder's title, such as Dr., Sir, or Mrs. A separator period (.) must precede the title.

  For example:

  BROWN/ROBERT S.DR
- If two Cardholder names are present in the Account Information Area on the same Card, encode in any of the following four formats:

  BROWN/ROBERT S or

  BROWN/AGNES T or

  BROWN/ROBERT AGNES or

  BROWN/ROBERT S.MR MRS
- If a Card has a company name present in the Account Information Area, in addition to a Cardholder name, encode the Cardholder name.

  For example:

Present in the Account Information Area:	ROBERT S. BROWN
	ALPHA COMPANY
Encoded on the magnetic stripe:	BROWN/ROBERT S

NOTA:

The subfields surname, initials or first name, and title may contain spaces. For example:

Present in the Account Information Area: RT REV ROBERT J SMITH

Encoded on the magnetic stripe: SMITH/ROBERT J.RT REV

3.5.4 Expiration Date

The following requirements apply for the encoded expiration date:

- The Card-read stripe must include the encoded Account's expiration date. Acceptable expiration date values are the following:

  Year 00–99

  Month 01–12
- The format for the encoded expiration date is YYMM to comply with ISO specifications.
- The encoded expiration date on Track 1 must be the same as the expiration date encoded on Track 2 and present in the Account Information Area.
- Do not encode the start date for dual dating, except as part of the Discretionary Data field on Track 1 and Track 2 of the magnetic stripe.

A Maestro or Cirrus Card must not use a maximum validity period of more than 20 years from the date of issuance or, for non-expiring Cards, the designated default value of 4912 (December 2049) must be used. For a Maestro or Cirrus Card issued in the Europe Region and using the Europay Security Platform (ESP) PIN Verification Value (PVV), the maximum validity period is the current year plus four (effectively a five-year validity period).

The expiration date of a Chip Card must not exceed the expiration date of any of the certificates contained within the chip. In the case of a non-expiring Chip Card:

1. The settings within the chip must force every Transaction online for authorization or decline the Transaction if online authorization is not possible;
2. The Chip Card must not contain an offline Card Authentication Method (CAM) certificate; and
3. The Issuer must utilize full EMV processing.

3.6 Tarjetas con Chip

Las Tarjetas con Chip, también conocidas como Tarjetas de circuito integrado o inteligentes, son Tarjetas de crédito o de débito que contienen chips de computadoras con memoria y capacidades interactivas y se pueden usar para identificar y guardar los datos adicionales del Tarjetahabiente, de la cuenta del Tarjetahabiente, o de ambos. Las Tarjetas con Chip pueden tener funcionalidad por contacto o ambas, funcionalidad por contacto o sin contacto.

Los Emisores de Tarjetas con Chip deben acatar todas las Normas aplicables, incluyendo, entre otras, las Normas establecidas en el manual *M/Chip Requirements* y otra documentación de M/Chip y las especificaciones de EMV.

El Emisor de una Tarjeta con Chip debe implementar el M/Chip como la aplicación de pago de EMV en la Tarjeta, de acuerdo con una especificación actual de la aplicación de la Tarjeta de M/Chip.

Una Tarjeta con Chip de contacto se puede emitir o volver a emitir bajo un Programa de Tarjetas en línea solamente (es decir, una "Tarjeta con chip de contacto en línea solamente"). Una Tarjeta con chip de contacto en línea solamente está configurada de modo que siempre requiere que la Terminal del POS obtenga una autorización en línea del Emisor para una Transacción con chip de contacto.

Con vigencia en las fechas descritas a continuación, el Emisor de una Tarjeta con Chip con contacto debe realizar un método de autenticación de la Tarjeta en línea (CAM en línea) de cada Transacción con Chip con contacto autorizada en línea por medio de la validación del Criptograma de Solicitud de Autorización (ARQC) contenido en el mensaje de Solicitud de Autorización/0100 o de Solicitud de Transacción Financiera/0200 y completar el DE 55, incluyendo un Criptograma de Respuesta de Autorización (ARPC), en el mensaje de Respuesta de Solicitud de Autorización/0110 o de Respuesta de Solicitud de Transacción Financiera/0210. Como alternativa, si el sistema de computadora principal del Emisor no apoya la validación del ARQC, el Emisor debe inscribirse en el Servicio de Validación Previa del Criptograma del M/Chip de MasterCard.

- Cualquier Emisor ubicado en la Región de Asia/Pacífico, Canadá, Europa, América Latina y el Caribe o Medio Oriente/Africa que no acata debe establecer un plan de acción de acatamiento a más tardar para el 1 de enero de 2015.
- Todos los Emisores ubicados en la Región de Asia/Pacífico, Canadá, Europa, América Latina y el Caribe o Medio Oriente/Africa deben estar en acatamiento a más tardar el 17 de abril de 2015.
- Todos los Emisores ubicados en la Región de Estados Unidos deben estar en acatamiento antes del 1 de octubre de 2015.

Los siguientes requisitos aplican a cualquier Tarjeta con Chip configurada para apoyar la autorización fuera de línea.

En esta región...	**Se requiere el apoyo a la DDA y la SDA no debe ser apoyada para las Tarjetas con Chip emitidas en o después de...**	**Se requiere el apoyo a la CDA para las Tarjetas con Chip emitidas en o después de...**
Región de Asia/Pacífico	16 de octubre de 2015	1 de enero de 2017
Región de Canadá	16 de octubre de 2015	1 de enero de 2017
Región de Europa	1 de enero de 2011	1 de enero de 2016
Región de América Latina y el Caribe	16 de octubre de 2015	16 de octubre de 2015
Región de Medio Oriente/Africa	16 de octubre de 2015	1 de enero de 2017
Región de Estados Unidos	Aplica a todas las Tarjetas con Chip	1 de enero de 2017

Aplican los siguientes requisitos en todas las Regiones:

- Las Tarjetas con Chip que apoyan la SDA como CAM fuera de línea deben vencer o ser reemplazadas a partir del 1 de enero de 2020; y
- Las Tarjetas con Chip que apoyan la DDA como el único CAM fuera de línea deben vencer o ser reemplazadas a partir del 1 de enero de 2022.

NOTA: Los emisores deben definir su prioridad de métodos de verificación del PIN dentro del chip. Se recomienda la verificación del PIN fuera de línea como la primera prioridad.

3.6.1 Chip Card Applications

All Payment Applications must be type-approved by MasterCard, prior to Chip Card production. Furthermore, the composition of the chip, operating system (if present), and the EMV application must have successfully passed a Compliance Assessment and Security Testing (CAST) security evaluation.

Issuers must define within the chip the preferred verification method for Point-of-Interaction (POI) Transactions. A non-Customer that personalizes Payment Applications acts on behalf of the Card Issuer and must conform to MasterCard security Standards.

Issuers using M/Chip 4 should refer to the *M/Chip Personalization Data Specifications and Profiles* and the *M/Chip 4 Version 1.1 Issuer Guide to Debit and Credit Parameter Management* for more information.

Issuers using M/Chip Advance should refer to the *M/Chip Advance Personalization Data Specifications* and the *M/Chip Advance—Issuer Guide* for more information.

3.6.1.1 Pruebas de Seguridad y Evaluación de Acatamiento

MasterCard ha establecido el proceso de CAST para ayudar a sus Emisores en la promoción de mejoras permanentes de las Normas de seguridad para la implementación de todas las Tarjetas con Chip de MasterCard. Los emisores solamente pueden emitir Tarjetas con Chip que han sido certificadas bajo el proceso CAST y aparecen en la lista de Productos Aprobados por las CAST (las Tarjetas con Chip que han experimentado una evaluación exitosa frente a las Pautas de Seguridad de las CAST utilizando un laboratorio de evaluación reconocido). Las Tarjetas permanecerán por lo general en la lista de Productos Aprobados por las CAST durante tres años desde la fecha de evaluación.

Antes de la producción, compra y distribución de las Tarjetas con Chip, los Emisores deben confirmar con sus proveedores que la Tarjeta con Chip estará en la lista de Productos Aprobados por las CAST durante el período previsto de emisión y adaptarán sus cantidades de adquisición según corresponda.

Para obtener información sobre las CAST, consulte el manual *Compliance Assessment and Security Testing Program* o comuníquese con el Departamento de Ayuda del Chip a chip_help@mastercard.com.

3.6.1.2 Proveedores de Chip de Circuito Integrado

Un Emisor debe obtener todos los chips de EMV para incrustarlos en una Tarjeta de un fabricante de chip de EMV que ha sido aprobado previamente por MasterCard.

MasterCard publica periódicamente una lista de fabricantes de chip de EMV aprobados en un *Boletín de Seguridad Global*. O para obtener más información, comuníquese con el Departamento de Ayuda de Chip en chip_help@mastercard.com.

3.6.2 Multiple Application Chip Cards

Any Card Program may reside on a chip, and any combination of Card Programs may reside together on a single Chip Card. All credit, debit, charge, and stored-value applications residing on a single Chip Card must be offered by, and are the responsibility of the Card Issuer.

Additionally, all other applications stored on a Chip Card by any Issuer, or any other party at an Issuer's request, must conform to all relevant technical specifications of MasterCard or its agent.

3.6.3 Use of M/Chip Card Application Specifications

Chip Card products that incorporate any implementation of the MasterCard M/Chip Card application specifications may only be used on MasterCard, Maestro, and Cirrus Cards and Access Devices, unless otherwise agreed in writing by MasterCard.

The M/Chip Card application specifications are available on MasterCard Connect™ in the *Chip Information Center*.

3.7 Contactless Cards and Payment Devices

MasterCard prohibits the encoding of the Cardholder name in the contactless chip of a contactless-enabled Card ("Contactless Card") or Contactless Payment Device that allows such information to be transmitted via the radio frequency (RF) contactless interface. This restriction applies to all newly issued and re-issued contactless-enabled Cards and Contactless Payment Devices.

Effective as of the dates described below, the Issuer of a Contactless Card or Contactless Payment Device must perform an online CAM for each online-authorized EMV Mode Contactless Transaction by validating the Authorization Request Cryptogram (ARQC) contained in the Authorization Request/0100 or Financial Transaction Request/0200 message. Alternatively, if the Issuer's host system does not support ARQC validation, the Issuer must be enrolled in the MasterCard M/Chip Cryptogram Pre-Validation Service.

- Any Issuer located in the Asia/Pacific, Canada, Europe, Latin America and the Caribbean, or Middle East/Africa Region that is not in compliance must establish a compliance action plan by 1 January 2015.
- All Issuers located in the Asia/Pacific, Canada, Europe, Latin America and the Caribbean, or Middle East/Africa Region must be in compliance by 17 April 2015.
- All Issuers located in the United States Region must be in compliance by 1 October 2015.

A Contactless Card or Contactless Payment Device with M/Chip functionality that is issued or re-issued in the Asia/Pacific, Canada, Europe, Latin America and the Caribbean, or Middle East/Africa Region:

- Must support CDA as the offline CAM, unless it supports online-only authorization of Contactless Transactions; and
- Must not support SDA as the offline CAM.

A Contactless Card or Contactless Payment Device with M/Chip functionality that is issued or re-issued in the United States Region:

- Must be configured to support both online and offline authorization of Contactless Transactions; and
- Must support CDA as the offline CAM and must not support SDA.

Refer to the *M/Chip Requirements* for additional details.

3.8 Mobile Payment Devices

There is no limitation on the type of account that may co-reside on the same Mobile Payment Device user interface, so long as such accounts are not linked, but rather exist independently and are accessed by a separate and distinct Payment Application hosted on the same or different user interfaces.

Mobile Payment Devices may support MasterCard contactless payment and/or Digital Secure Remote Payment (DSRP) functionality. If an Issuer chooses to add this functionality to a Secure Element (SE)-based Mobile Payment Device, the application software, personalization data, and all other aspects of the functionality must comply with the requirements set forth in the Standards, including but not limited to the following as may be published by MasterCard from time to time:

- *Mobile MasterCard PayPass User Interface Application Requirements*,
- *M/Chip Mobile Issuer Implementation Guide v1.1*,
- the contactless branding Standards, and
- any other applicable technical specifications.

For Mobile Payment Devices supporting MasterCard contactless payment or DSRP functionality that do not use an SE, Issuers should refer to the MasterCard Cloud-Based Payment (MCBP) documentation.

Issuers should also refer to the mobile payment security guidelines set forth in the *Security Guidelines for Mobile Payment Solutions*.

The SE must be CAST-approved and have received a mobile payment certificate number (MPCN). Issuers may choose a CAST-approved SE (with corresponding MPCN) from the list published on MasterCard Connect. The Mobile Payment Device itself does not undergo a CAST approval. Prior to issuance of the SE-based Mobile Payment Device, the Payment Application must also pass the functional and security testing program, for which a letter of approval will be issued by MasterCard.

For information regarding CAST, refer to the *Compliance Assessment and Security Testing Program* manual. For information regarding a letter of approval, refer to the *M/Chip Mobile Issuer Implementation Guide v1.1*.

3.9 Métodos de Verificación del Tarjetahabiente del Dispositivo del Consumidor

Las tecnologías de autenticación del consumidor usadas en los dispositivos del consumidor, tal como las computadoras personales, tabletas, teléfonos móviles y relojes, están diseñadas para verificar a una persona como usuario autorizado del dispositivo en uno o más de los siguientes:

- "Algo que sé"—Información seleccionada y que se pretende que sepa solamente esa persona, tal como un código de acceso o patrón
- "Algo que soy"—Una característica física que se puede traducir en información biométrica con el fin de identificar exclusivamente a una persona, tal como un rostro, huella o pulso
- "Algo que tengo"—Información que pretende identificar exclusivamente un dispositivo particular del consumidor

Cualquier tecnología de autenticación del consumidor debe ser aprobada por MasterCard como un "CVM calificado por MasterCard" antes de que pueda usarse como Método de Verificación del Tarjetahabiente del Dispositivo del Consumidor (CDCVM) para procesar una Transacción.

3.9.1 Calificación de MasterCard de los CVM del Dispositivo del Consumidor

Antes de que un Cliente (tal como un Emisor o Solicitante de Token de Billetera) pueda usar, como un CDCVM, una tecnología de autenticación del consumidor conectada con la funcionalidad de pago de un tipo particular de Dispositivo de Acceso (de un fabricante y modelo específico), el Cliente debe enviar la tecnología a MasterCard para la certificación y para efectuar pruebas.

La certificación y pruebas de un CDCVM propuesto se efectúan mediante o en nombre de MasterCard, de acuerdo con los requisitos de MasterCard y a expensas del Cliente o tercero, según corresponda. La certificación requiere que tanto las pruebas de seguridad como las operativas sean exitosas.

Después de completar la certificación y las pruebas, MasterCard, a su discreción, puede aprobar una tecnología de autenticación del consumidor propuesta como "CVM calificado por MasterCard". La información del informe de resumen sobre dicha certificación y resultados de las pruebas y la conclusión exitosa de las pruebas de certificación se pueden divulgar a los Clientes por medio de MasterCard o un tercero que efectúa la certificación y las pruebas en nombre de MasterCard. Cualquier propuesta de actualización, cambio o modificación de la tecnología de autenticación del consumidor que pueda tener impacto sobre la funcionalidad o seguridad del CDCVM se debe enviar a MasterCard para la certificación y para efectuar pruebas como una nueva tecnología de autenticación del consumidor propuesta. MasterCard se reserva el derecho de cambiar los requisitos para el CVM calificado por MasterCard en cualquier momento y de cambiar o establecer requisitos nuevos de certificación y pruebas.

3.9.2 Funcionalidad de CDCVM

MasterCard exige pruebas y certificación de cada una de las siguientes funcionalidades de CDCVM propuestas antes del uso para efectuar una Transacción:

1. **Funcionalidad de Autenticación Compartida**—El método usado para verificar las credenciales establecidas por una persona en relación con el uso del Dispositivo de Acceso o de una Billetera Digital en el Dispositivo de Acceso también es el método usado como CDCVM predeterminado para las Transacciones que incluyen Cuentas a las que se obtiene acceso por medio del Dispositivo de Acceso.
2. **Resultado del CVM con Base en la Autenticación y el Consentimiento Explícito**—La Aplicación de Pago en el Dispositivo de Acceso analiza el resultado combinado de la autenticación y las acciones de consentimiento y configura los resultados del CDCVM de manera acorde. Tanto la autenticación del Tarjetahabiente como el consentimiento explícito del Tarjetahabiente deben ocurrir antes de que la Aplicación de Pago complete la Transacción, de la siguiente manera:
    a. **Autenticación del tarjetahabiente**—El Dispositivo de Acceso puede pedir al Tarjetahabiente que realice la acción del CDCVM al momento de la Transacción, o el CDCVM puede consistir de una autenticación persistente o de una autenticación prolongada en la cual se inicia la acción del CDCVM y también pueda completarse antes de que ocurra la Transacción, según se describe en las secciones 3.9.3 y 3.9.4.
    b. **Consentimiento Explícito del Tarjetahabiente**—El Tarjetahabiente toma una acción específica aprobada por el Emisor que sirve para confirmar que el Tarjetahabiente intenta que se efectúe una Transacción. Esto debe consistir de una acción que incluye que el Dispositivo de Acceso está separado del acto de tocar el Dispositivo de Acceso en la Terminal de POS; por ejemplo, hacer clic en un botón.
3. **Dispositivos del Consumidor Conectados**—Si dos o más dispositivos bajo el control de un Tarjetahabiente se pueden conectar o vincular para proporcionar una funcionalidad de pago común, de modo que cada dispositivo pueda ser un Dispositivo de Acceso para la misma Cuenta, entonces deberá tener lugar el consentimiento del Tarjetahabiente en el Dispositivo de Acceso usado para efectuar la Transacción.
4. **Integridad del Dispositivo**—Después del inicio y de continuar con la autenticación del Tarjetahabiente, el uso del CDCVM debe depender de sólidas verificaciones de la integridad del dispositivo. Ejemplos incluyen las verificaciones de la integridad de ejecución del dispositivo, la ratificación del dispositivo a distancia o una combinación de ambas y las verificaciones para asegurar que la velocidad prolongada del CVM está intacta; por ejemplo, la funcionalidad de bloqueo del dispositivo no fue inhabilitada.

Los requisitos de la funcionalidad del CDCVM aplican solamente en la medida en que un CVM es solicitado por el Comercio o por la Terminal o requerida por el Emisor para completar una Transacción.

3.9.3 Autenticación Persistente

La autenticación persistente significa que la autenticación de una persona como Tarjetahabiente ocurre de forma continua durante el funcionamiento del Dispositivo de Acceso

por parte de una persona, por lo general, a través del contacto continuo o del control biométrico (por ejemplo, el control del pulso).

MasterCard exige pruebas y certificación de la funcionalidad de CDCVM propuesta para la autenticación persistente con respecto a lo siguiente:

1. Se utiliza un mecanismo de verificación de persistencia calificado por MasterCard para detectar un cambio en la persona que usa el dispositivo;
2. El dispositivo en el cual se inicia la autenticación puede detectar sin interrupción que la persona autenticada permanece cerca de dicho dispositivo o de cualquier dispositivo conectado con el cual comparte la funcionalidad de pago común;
3. El dispositivo tiene la capacidad de pedir el consentimiento explícito del Tarjetahabiente (por ejemplo, al solicitar que el Tarjetahabiente haga clic en un botón o toque el dispositivo) antes de que se pueda efectuar una Transacción; y
4. La tecnología de autenticación del consumidor acata las Normas de MasterCard.

3.9.4 Autenticación Prolongada

La autenticación prolongada ocurre cuando la autenticación de un Tarjetahabiente (por ejemplo, el ingreso y verificación positiva de un código de acceso) permanece válido para un período de tiempo (el "período abierto") y, durante ese período abierto, no se solicita ni se requiere ninguna autenticación más para que el Tarjetahabiente efectúe una Transacción.

MasterCard exige pruebas y certificación de la funcionalidad de CDCVM propuesta para la autenticación prolongada con respecto a los siguiente:

1. La Billetera Digital o Aplicación de Pago que reside en el dispositivo puede pedir una nueva autenticación del Tarjetahabiente con base en los límites de parámetros definidos;
2. El dispositivo puede pedir el formulario de consentimiento explícito del Tarjetahabiente aprobado por el Emisor (por ejemplo, al solicitar que el Tarjetahabiente haga clic en un botón o toque el dispositivo) antes de que se pueda efectuar una Transacción;
3. El período abierto de la autenticación prolongada de un Tarjetahabiente puede ser compartido por los dispositivos del consumidor conectados o vinculados que son Dispositivos de Acceso para la misma Cuenta, siempre que los Dispositivos de Acceso estén cerca uno de otro; y
4. La tecnología de autenticación del consumidor acata las Normas de MasterCard.

3.9.5 Cómo Mantener el Estado del CVM Calificado por MasterCard

MasterCard puede exigir pruebas adicionales de un CDCVM calificado por MasterCard como condición para que el CDCVM permanezca como un CVM calificado por MasterCard; dicho requisito puede surgir, a modo de ejemplo, entre otros, en el caso de cualquier cambio tecnológico, de software, hardware, operativo u otro que pueda tener impacto, de forma directa o indirecta, en la seguridad u otra funcionalidad del CDCVM.

MasterCard se reserva el derecho de retirar el estado del CVM calificado por MasterCard con respecto a un CDCVM en cualquier momento si MasterCard tiene algún motivo para creer que la seguridad del CDCVM no es suficiente. MasterCard notificará a los Clientes si se retira un estado del CVM calificado de MasterCard. Después de la publicación de dicho aviso por

parte de MasterCard, un Cliente debe, de forma inmediata, dejar de ofrecer o de permitir el uso de dicha tecnología de autenticación del consumidor como un CVM.

3.9.6 Responsabilidades del Emisor

Antes de permitir que un Tarjetahabiente obtenga acceso a una Cuenta por medio de un Dispositivo de Acceso que usa un CDCVM para las Transacciones, el Emisor debe:

1. Confirmar que el CDCVM es un CVM Calificado por MasterCard;
2. Aprobar los formularios específicos permitidos de la autenticación del Tarjetahabiente y del consentimiento explícito del Tarjetahabiente que se completan en relación con el CDCVM;
3. Aprobar todos los límites de parámetros aplicables que se usan para determinar cuándo vence la autenticación de un Tarjetahabiente. Para la autenticación prolongada, dichos límites deben consistir de al menos uno de los siguientes (el que ocurra primero):

    a. El período abierto finaliza, el cual no puede superar cinco minutos seguidos;
    b. Se alcanza un número máximo de Transacciones, que no puede superar tres (3) Transacciones; o
    c. Se alcanza un volumen de la Transacción máximo acumulado que no puede superar US$150 o el equivalente en la moneda local (si se encuentra en el país donde se emitirán los Dispositivos de Acceso, es común el apoyo de MCL 3.0 y CDCVM por parte de las Terminales con capacidad sin contacto).

    La configuración de un límite de parámetros que supera cualquiera de los límites máximos estipulados anteriormente exige la aprobación expresa previa de MasterCard.

3.9.7 Uso de un Proveedor

Cualquier convenio que un Cliente firme con un proveedor para la provisión de los servicios de CDCVM debe incluir el acuerdo expreso del proveedor de garantizar y controlar el uso de la información personal y debe acatar todas las Normas aplicables.

3.10 Código de Validación de la Tarjeta (CVC)

El CVC es una característica de seguridad con componentes identificados en otros lugares de este manual. El uso de los CVC dificulta a los falsificadores modificar Tarjetas y volver a usarlas con fines fraudulentos.

NOTA: El CVC 1 y el CVC 2 son características de seguridad obligatorias para todas las Tarjetas MasterCard.

El CVC 1 debe estar codificado en las Pistas 1 y 2, en tres posiciones contiguas en el campo de Datos Discrecionales de la banda magnética de todas las Tarjetas MasterCard.

Las Tarjetas Maestro y Cirrus emitidas o reemitidas el 11 de enero de 2013 o posteriormente y que tengan un PAN de 16 dígitos o menos, deben apoyar el CVC 1 en la banda magnética y el CVC del Chip en el campo de los Datos Equivalentes de la Pista 2.

El CVC con Chip debe estar codificado en el campo de Datos Equivalentes de la Pista 2 en tres posiciones contiguas dentro del campo de Datos Discrecionales del chip en todas las Tarjetas con Chip y debe ser diferente al valor del CVC 1 codificado en la banda magnética.

Todos los Emisores de Tarjetas con Chip, incluyendo aquellos que utilizan el Servicio de Conversión de Chip a Banda Magnética, deben utilizar valores diferentes para el CVC 1 y el CVC con Chip para todas las Tarjetas nuevas y reemitidas.

Lo siguiente aplica a las Tarjetas con capacidad sin contacto ("Tarjetas Sin Contacto") y a los Dispositivos de Pago Sin Contacto:

- Todos los Dispositivos de Pago Sin Contacto y las Tarjetas Sin Contacto de perfil de banda magnética deben generar un CVC 3 dinámico.
- Todos los Dispositivos de Pago Sin Contacto y las Tarjetas de M/Chip Sin Contacto emitidas antes del 1 de enero de 2010 que son capaces de efectuar una Transacción Sin Contacto de Modo de Banda Magnética deben ser codificados ya sea con un CVC 3 estático o deben ser capaces de generar un CVC 3 dinámico.
- Todos los Dispositivos de Pago Sin Contacto y las Tarjetas de M/Chip Sin Contacto emitidas el 1 de enero de 2010 o posteriormente y que son capaces de efectuar una Transacción Sin Contacto de Modo de Banda Magnética deben generar un CVC 3 dinámico.

Consulte *M/Chip Requirements* para obtener detalles adicionales.

Consulte el Apéndice A para obtener los requisitos de formato de datos de la pista, formato y contenidos. Consulte la sección 3.10.5 para conocer los métodos de cálculo del CVC.

Consulte *M/Chip Requirements* para obtener información acerca del CVC del Chip.

Consulte el manual *M/Chip Processing Services—Service Description* para obtener información sobre el Servicio de Conversión de Chip a Banda Magnética.

3.10.1 Requisitos del Emisor para el CVC 1

Los Emisores de MasterCard deben:

- Codificar el CVC1 en las Pistas 1 y 2
- Verificar el CVC 1 codificado cuando están procesando una solicitud de autorización por lectura de Tarjeta

El Emisor verifica el valor del CVC 1 de los datos de lectura de la Tarjeta según se transmiten en la solicitud de autorización durante el proceso de autorización en línea. La computadora principal del Emisor puede desempeñar la verificación.

NOTA: Los Emisores deben realizar la certificación para validar el valor del CVC 1 durante el proceso de autorización y para señalar los errores de validación del CVC 1. Para obtener más información, consulte el Capítulo 4 del *Manual de Autorización*.

Cuando el sistema del Emisor se interrumpe o no está disponible, el Servicio del Procesamiento Stand-In proporciona una respuesta de solicitud de autorización. Si un Emisor está inscrito para la verificación del CVC 1, el Servicio del Procesamiento Stand-In lleva a cabo una prueba adicional para verificar que el valor del CVC 1 sea válido.

MasterCard puede exigir la participación en la verificación del CVC 1 en el Servicio del Procesamiento Stand-In para un Emisor con 35 puntos base de Transacciones autorizadas por medio del procesamiento Stand-In y con importante actividad de falsificaciones dentro de un trimestre calendario. Para obtener más información, consulte el Capítulo 6 del *Manual de Autorización*.

3.10.2 Requisitos del Emisor para el CVC 2

Los Emisores deben verificar el valor del CVC 2 cuando lo proporciona el Comercio y lo transmite el Adquiriente en el Elemento de Datos (DE) 48 (Datos Adicionales—Uso Privado), elemento secundario 92 (CVC 2) del mensaje de Solicitud de Autorización/0100 o del mensaje de Solicitud de Transacción Financiera/0200. Los emisores deben verificar el valor del CVC 2 al proporcionar un código de respuesta de CVC 2 válido de M (CVC 2 válido [coincide]), N (CVC 2 inválido [no coincide]), o de P (CVC 2 no procesado—el Emisor no está disponible temporalmente) en el DE 48, elemento secundario 87 (Resultado del Código de Validación de la Tarjeta) del mensaje de Respuesta de Solicitud de Autorización/0110 o del mensaje de Respuesta de Solicitud de Transacción Financiera/0210.

Para las Transacciones Nacionales de POS de Maestro que ocurren dentro del Reino Unido, Irlanda y Francia solamente, aplica lo siguiente:

- Si un Emisor recibe datos del CVC 2 en una solicitud de autorización y estos son inválidos (por ejemplo, el DE 48, elemento secundario 92 [CVC 2] no está en blanco y los datos no coinciden con los datos que se encuentran en los registros del Emisor) se debe rechazar la solicitud de autorización.
- Si se aprueba una solicitud de autorización con datos del CVC 2 inválidos, el Emisor no puede utilizar un código de motivo de mensaje relacionado con fraude para contracargar la Transacción.

3.10.3 Requisitos del Emisor para el CVC 3

El Emisor debe habilitar un CVC 3 dinámico en el chip sin contacto para todas las Transacciones Sin Contacto de perfil de banda magnética efectuadas por Tarjetas con Chip Sin Contacto de perfil de banda magnética o Dispositivos de Pago Sin Contacto.

Todas las nuevas Tarjetas con Chip con capacidad sin contacto y Dispositivos de Pago Sin Contacto emitidos el 1 de enero de 2010 o posteriormente, capaces de efectuar Transacciones Sin Contacto de perfil de banda magnética deben generar un CVC 3 dinámico.

El Emisor debe verificar el valor del CVC 3 y proporcionar el resultado en la respuesta cuando procesa la autorización recibida de una Transacción Sin Contacto.

3.10.4 Requisitos del Adquiriente para el CVC 2

Cuando el Comercio proporciona el valor del CVC 2, el Adquiriente debe incluir el valor del CVC 2 en el DE 48, elemento secundario 92 del mensaje de Solicitud de Autorización/0100 o del mensaje de Solicitud de Transacción Financiera/0200. El Adquiriente también es responsable de asegurarse de que el Comercio reciba el código de respuesta del CVC 2 proporcionado por el Emisor en el DE 48, elemento secundario 87 del mensaje de Respuesta

de Solicitud de Autorización/0110 o del mensaje de Respuesta de Solicitud de Transacción Financiera/0210.

Todas las Transacciones de juegos de azar que no son cara a cara realizadas con una Tarjeta MasterCard deben incluir el valor del CVC 2 en el DE 48, elemento secundario 92 del mensaje de Solicitud de Autorización/0100.

3.10.5 Métodos de Cálculo del CVC

El Emisor puede calcular el CVC 1, el CVC 2 y el CVC con Chip mediante uno de dos métodos:

- **Cálculo propio del Emisor**—el cual le da la opción al Emisor para obtener el CVC por lenguaje algorítmico.
- **Software de Norma de Encriptado de Datos (DES)**—donde el Emisor puede hacer el cálculo por medio de una aplicación del software de DES dentro de un sistema de computadora principal o por medio del uso de un módulo de seguridad resistente a alteraciones (TRSM).

Los Emisores que eligen el método del software de la DES deben usar el procedimiento de algoritmo de la DES para generar el CVC 1, CVC 2 y el CVC con Chip.

El procedimiento de algoritmo de la DES se describe a continuación y también se publica en los siguientes documentos:

- ANSI X3.92-1981 *American National Standard, Data Encryption Algorithm [Normas Nacionales Americanas, Algoritmo de Encriptado de Datos]*
- ISO/IEC 18033-3:2010, *Information technology—Security techniques—Encryption algorithms—Part 3: [Tecnología de la Información—Técnicas de seguridad—Algoritmos de Encriptado— Parte 3:] Block ciphers [Cifrados por Bloques]* (consulte el Anexo A)

El algoritmo del método de la DES genera el CVC 1 de tres dígitos para el campo de Datos Discrecionales de la Pista 1 y de la Pista 2. El Emisor también usa este método para desarrollar el CVC 2 de tres dígitos y el CVC con Chip. Este procedimiento de algoritmo aplica solamente a los Emisores que implementan el proceso de generación del CVC en sus sistemas de computadoras principales.

MasterCard requiere dos claves de DES criptográficas de 64 bits para usar en el proceso de generación. Un Emisor puede utilizar las mismas dos claves DES de 64 bits para generar el CVC 1, el CVC 2 y el CVC con Chip (pero no el CVC 3) siempre y cuando se utilicen los códigos de servicio separados. No se deben compartir las mismas claves entre Emisores múltiples, tal como cuando los Emisores utilizan un Proveedor de Servicios común para el procesamiento del CVC 1, CVC 2 y CVC con Chip.

MasterCard desalienta enérgicamente a que los Emisores usen un valor del CVC 2 de "000".

El procedimiento del algoritmo de la DES se efectúa siguiendo los ocho pasos a continuación:

1. Si el número de cuenta primario (PAN) excede los 16 dígitos, extraiga los últimos 16 dígitos del PAN.

2. Construya una cadena de bits ordenando en serie (de izquierda a derecha) la secuencia de valores de 4 bits (o nibbles), cada uno de los cuales es la representación binaria de un dígito numérico en los Elementos de Datos del CVC, en el orden indicado en la Tabla 3.2:

   NOTA: El Emisor debe efectuar cálculos independientes para producir cada valor del CVC.

Tabla 3.2—Elementos de Datos del CVC

Para el CVC 1	Para el CVC 2	Para el CVC con Chip	Longitud (toda)
Resultado del Paso 1	Resultado del Paso 1	Resultado del Paso 1	16
Fecha de vencimiento de la tarjeta (según aparece en la codificación de la Pista 2).	Fecha de vencimiento de la tarjeta (según aparece en el Area de Información de la Cuenta en el frente de la Tarjeta)	Fecha de vencimiento de la tarjeta (según aparece en la codificación de los Datos Equivalentes de la Pista 2)	4
El valor del código de servicio NO debe ser "000"	El valor del código de servicio debe ser "000"	El valor del código de servicio debe ser "999"	3
Total			23

3. Aplique la ISO/IEC 9797-1 "Algoritmo 3 de MAC", "Método de Relleno 1" a la cadena creada en el Paso 2, utilizando dos claves DES independientes, para producir un resultado de 8 bytes.
4. Del resultado del Paso 3, de izquierda a derecha, un nibble a la vez, extraiga todos los nibbles que corresponden a los dígitos numéricos (0–9); justifique a la izquierda estos dígitos en un campo de 16 posiciones.
5. Del resultado del Paso 3, de izquierda a derecha, un nibble a la vez, extraiga todos los nibbles que correspondan a los caracteres hexadecimales (A–F). Para compensar el hexadecimal, reste 10 de cada dígito hexadecimal extraído.
6. Concatene los dígitos resultantes del Paso 5 a la derecha de los dígitos extraídos en el Paso 4.
7. Determine el CVC para los primeros tres dígitos que se encuentran más a la izquierda de la cadena decimal creada en el Paso 6.
8. Ejecute el programa tres veces, una por cada CVC, utilizando los elementos de datos del CVC indicados en la Tabla 3.2.

[1] Para el OBKM, el formato de la fecha de vencimiento de la Tarjeta puede presentarse ya sea como AAMM o MMAA. Consulte las *On-Behalf Key Management (OBKM) Interface Specifications [Especificaciones de la Interfaz del Manejo de Claves En Nombre de (OBKM)]*.

[2] El resultado del Paso 1 es de 16 dígitos de longitud. La cadena resultante refleja 23 dígitos (16+4+3) y es de 92 bits de longitud.

3.11 Códigos de Servicio

El código de servicio, un número de tres dígitos que acata la ISO 7813 (Tarjetas de Identificación—Tarjetas de Transacción Financiera), está codificado en la Pista 1 y Pista 2 de la banda magnética de una Tarjeta e indica a la terminal que lee la banda magnética los parámetros de aceptación de la Transacción de la Tarjeta. Cada dígito del código de servicio representa un elemento distinto de la política del Emisor sobre la aceptación de la Transacción. Sin embargo, no todas las combinaciones de dígitos válidos constituyen un código de servicio válido, ni todas las combinaciones de código de servicio son válidas para todos los Programas de Tarjetas. Los emisores pueden codificar solamente un código de servicio en las Tarjetas y el mismo valor debe ser codificado en la Pista 1 y la Pista 2 en sus respectivas posiciones designadas.

Los códigos de servicio proporcionan a los Emisores flexibilidad para definir los parámetros de aceptación de Tarjetas y proporcionan a los Adquirientes la capacidad de interpretar las preferencias de aceptación de Tarjetas del Emisor para todas las condiciones del POI.

Los códigos de servicio aplican solamente a las Transacciones por lectura de banda magnética. En el caso de las Tarjetas con Chip utilizadas en las Terminales de POS Híbridas, la Terminal de POS Híbrida utiliza los datos codificados en el chip para completar la Transacción.

NOTA:

Un valor de 2 ó 6 en la posición 1 del código de servicio indica que un chip está presente en una Tarjeta que contiene la aplicación de MasterCard que está presente en la banda magnética.

3.11.1 Información del Emisor

Actualmente, MasterCard recomienda usar el valor del código de servicio 101 (Tarjeta internacional, autorización normal, verificación normal del Tarjetahabiente, sin restricciones) para la mayoría de las aplicaciones de Tarjetas. Para obtener más información, consulte la Tabla 3.3 de este capítulo.

Para una Tarjeta Maestro, el Emisor debe usar los siguientes valores en el código de servicio:

- Un valor de 1 ó 2 en la posición 1;
- Un valor de 0 ó 2 (recomendado) en la posición 2; y
- Un valor de 0, 1 ó 6 en la posición 3. Si se usa un valor de 1 ó 6, el Emisor debe aceptar las Transacciones que no contienen los datos del PIN.

Para una Tarjeta Cirrus (en ATM solamente), el Emisor debe usar los siguientes valores en el código de servicio:

- Un valor de 1 ó 2 en la posición 1;
- Un valor de 0 ó 2 en la posición 2; y
- Un valor de 0, 1 ó 3 (recomendado) en la posición 3.

Un Emisor de Tarjeta Debit MasterCard no debe codificar un valor de 5 ó 7 en la posición 3 del código de servicio.

Un Emisor de Tarjeta MasterCard Electronic debe codificar un valor de 2 (se requiere autorización positiva en línea) en la posición 2 del código de servicio.

Los emisores pueden usar códigos de servicio para apoyar la emisión de aplicaciones de ICC y los requisitos de PIN.

A los efectos de la prevención de fraude, se recomienda encarecidamente a los Emisores establecer parámetros de autorización que rechacen cualquier Transacción que contenga los valores de código de servicio inválidos de 000 ó 999.

3.11.2 Información del Adquiriente

Los adquirientes deben asegurarse de que sus Terminales Híbridas no rechacen el procesamiento completo de una Transacción debido únicamente al código de servicio codificado en la banda magnética.

No se exige a los Adquirientes actuar sobre los códigos de servicio en este momento a menos que:

- Un valor de 2 ó 6 está presente en la posición 1 del código de servicio para una Aplicación de Pago de MasterCard, Maestro o Cirrus. La Terminal Híbrida primero debe intentar procesar la Transacción como una Transacción con chip; o
- La Terminal está ubicada en la Región de Europa y tiene capacidad de lectura de banda magnética. y un valor de 2 está presente en la posición 2 del código de servicio para una Aplicación de Pago de MasterCard. El Adquiriente debe asegurarse de que la autorización se obtenga antes de que el Comercio complete una Transacción por lectura de banda magnética.

3.11.3 Códigos de Servicio Válidos

La tabla 3.3 define los valores del código de servicio para las Aplicaciones de Pago de MasterCard, MasterCard Electronic, Maestro y Cirrus y cada posición del código de servicio de tres dígitos.

NOTA: Los códigos de servicio tienen una longitud de tres posiciones. Para identificar los valores del código de servicio válidos, combine los números válidos para cada una de las tres posiciones en esta tabla. El valor 000 no es un código de servicio válido y no debe estar codificado en la banda magnética de las tarjetas MasterCard, MasterCard Electronic, Maestro o Cirrus.

Tabla 3.3—Valores del Código de Servicio

Definición	Posición 1	Posición 2	Posición 3
Tarjeta Internacional	1		

Definición	Posición 1	Posición 2	Posición 3
Tarjeta Internacional—Tarjeta de Circuito Integrado	2		
Uso Nacional Solamente	5		
Uso Nacional Solamente—Tarjeta de Circuito Integrado	6		
Tarjeta de Marca Privada o Tarjeta Propia	7		
Autorización Normal		0	
Se Requiere Autorización Positiva En Línea		2	
Se requiere el PIN			0
Verificación Normal del Tarjetahabiente, Sin Restricciones			1
Verificación Normal del Tarjetahabiente—Solamente bienes y servicios en el Punto de Venta (sin provisión de efectivo)			2
ATM Solamente, se requiere el PIN			3
Se requiere el PIN—Bienes y servicios solamente en el Punto de Venta (sin provisión de efectivo)			5
Indicación para ingresar el PIN si hay Teclado para marcar el PIN			6
Indicación para ingresar el PIN si hay Teclado para marcar el PIN—Solamente bienes y servicios en el Punto de Venta (sin provisión de efectivo)			7

3.11.4 Información Adicional del Código de Servicio

La siguiente información explica los valores del código de servicio en la Tabla 3.3.

- Autorización normal es una Transacción autorizada de acuerdo con las reglas establecidas que rigen las Transacciones en el POI.
- Los códigos de servicio Se Requiere Autorización Positiva En Línea (valor de 2 en la posición 2) indican que se debe solicitar una autorización electrónica para todas las Transacciones. Este valor de código de servicio se debe usar en las tarjetas MasterCard Electronic™, pero es opcional para las tarjetas MasterCard Sin Grabado al Relieve.
- Verificación normal del Tarjetahabiente indica que el CVM debe realizarse de acuerdo con las reglas establecidas que rigen la verificación del Tarjetahabiente en el POI.

- Los códigos de servicio relacionados con la ICC (valor de 2 ó 6 en la posición 1) se permiten solamente en Tarjetas con Chip que contienen un tipo de Aplicación de Pago de MasterCard, Maestro, o Cirrus aprobada por MasterCard o su agente.
- Los códigos de servicios relacionados con la ICC (valor de 2 ó 6 en la posición 1) no se pueden utilizar para las aplicaciones independientes (de efectivo) de valor almacenado que se encuentran en las tarjetas de MasterCard, Maestro, o Cirrus En estos casos, se debe colocar un valor 1 en la primera posición.
- Los códigos de servicio para Uso Nacional Solamente (valor de 5 ó 6 en la posición 1) se permiten solo en Tarjetas de Uso Nacional Solamente aprobadas por MasterCard. Esto incluye los códigos de servicio relacionados con el PIN en las Tarjetas de **Uso Nacional Solamente** (por ejemplo, 506) controladas por el reglamento del procesamiento del PIN local.
- Los códigos de servicio de marca privada o propia (valor de 7 en la posición 1) en las Tarjetas que contienen un BIN válido de MasterCard se permiten solamente en Tarjetas de marca privada o propia aprobadas por MasterCard.

Los Emisores no pueden usar códigos de servicio relacionados con el PIN para los Programas de Tarjetas a menos que MasterCard haya aprobado el uso indicado de un PIN.

Capítulo 4 Terminal and PIN Security Standards

This chapter may be of particular interest to Issuers of Cards that support PIN as a Cardholder verification method (CVM) and Acquirers of Terminals that accept PIN as a CVM. Refer to the applicable technical specifications and the Transaction Processing Rules manual for additional Terminal and Transaction processing requirements relating to the use of a PIN.

4.1 Números de Identificación Personal (PIN)

Un Emisor debe proporcionar a cada uno de sus Tarjetahabientes un número de identificación personal (PIN) junto con la emisión de la Tarjeta MasterCard, u ofrecer al Tarjetahabiente la opción de recibir un PIN. El Emisor debe proporcionar un PIN al Tarjetahabiente junto con la emisión de las Tarjetas Maestro y Cirrus. El PIN permite a los Tarjetahabientes obtener acceso a la Red de ATM de MasterCard® que acepta las marcas MasterCard®, Maestro® y Cirrus® y realizar Transacciones en dispositivos de terminal activada por el Tarjetahabiente (CAT) 1, en los Comercios de Maestro y en las Terminales de Punto de Venta (POS) Híbridas.

El Emisor deberá consultar las pautas para el manejo de claves y del PIN descritas en *Issuer PIN Security Guidelines*.

El Adquiriente debe acatar la edición más reciente de los siguientes documentos, disponible en www.pcisecuritystandards.org:

- *Payment Card Industry PIN Security Requirements*
- *Payment Card Industry POS PIN Entry Device Security Requirements*
- *Payment Card Industry Encrypting PIN Pad Security Requirements*

4.2 Selección y Uso del PIN

Un Emisor es responsable de generar, almacenar, procesar y apoyar el cambio de los PIN. Como parte de esta función, el Emisor debe apoyar y controlar el PIN durante su ciclo de duración.

Algunos métodos estandarizados de generación del PIN acatan la norma (ISO) 9564 de la Organización Internacional para la Estandarización (ISO) y permiten la verificación del PIN en plataformas sin la necesidad de almacenar el PIN. Estos métodos eliminan la necesidad de un almacenamiento seguro expandido y permiten que la verificación del PIN se base en la computación de un valor en lugar de comparar el PIN desencriptado contra un valor almacenado.

El PIN puede ser generado por el Emisor o seleccionado por el Tarjetahabiente. MasterCard recomienda enfáticamente que los Emisores proporcionen la oportunidad a los Tarjetahabientes de reemplazar el PIN asignado con un PIN seleccionado por ellos mismos.

Los PIN deben ser numéricos, alfabéticos o alfanuméricos. El PIN debe tener al menos cuatro y no más de seis caracteres de longitud, excepto para las Tarjetas emitidas en las Regiones de Canadá y Estados Unidos, el PIN puede tener hasta 12 caracteres de longitud. Si se genera un PIN alfabético o alfanumérico, el Emisor debe avisar al Tarjetahabiente que muchos de los dispositivos de entrada del PIN solamente contienen caracteres numéricos y deben proporcionar el equivalente numérico de los primeros seis caracteres alfabéticos del PIN.

Un emisor no debe generar, ni permitir a sus Tarjetahabientes seleccionar un PIN que incluya las letras Q o Z.

Los emisores deben consultar la *Issuer PIN Security Guidelines* para obtener más información sobre la selección del PIN del Tarjetahabiente y del Emisor.

4.3 PIN Verification

An Issuer must be capable of verifying PINs based on a maximum of six characters. The Issuer may use the PIN verification algorithm of its choice.

If a Card is encoded with a PIN Verification Value (PVV), then the Issuer may use the MasterCard PIN verification service for authorization processing. If a proprietary algorithm is used for the PVV calculation or the PVV is not encoded on the Card, then PIN verification will not be performed on a Transaction authorized by means of the Stand-In Processing Service.

A Customer in a Region other than the Europe Region may refer to "PIN Processing for Non-Europe Region Customers" in the *Authorization Manual*, Chapter 9, "Authorization Services Details" for more information about the MasterCard PIN verification service, in which the MasterCard Network performs PIN verification on behalf of Card Issuers. Europe Region Customers should refer to Chapter 12, "PIN Processing for Europe Region Customers," of the *Authorization Manual*.

Refer to "PIN Generation Verification" in *Single Message System Specifications*, Chapter 6, "Encryption" for more information about PIN verification that the MasterCard Network performs directly for Debit MasterCard Card and Maestro and Cirrus Card Issuers, and the two PIN verification methods (IBM 3624 and ABA) that the PIN verification service supports. The ANSI format of PIN block construction is also described in that chapter.

4.4 PIN Authorization Requests

Refer to the following manuals for additional support of Transactions that contain a PIN in the Authorization Request/0100 message:

- *Authorization Manual*, Chapter 9—Authorization Services Details
- *Customer Interface Specification*, Chapter 5—Program and Service Format Requirements

4.5 Cifrado del PIN

Todos los Clientes y sus agentes que realizan el procesamiento de Transacciones con PIN deben acatar los requisitos de seguridad para el cifrado del PIN especificados en el documento *Payment Card Industry PIN Security Requirements*.

Todos los Emisores y sus agentes que realizan el procesamiento del PIN deberán además consultar el documento *Issuer PIN Security Guidelines* referente al cifrado del PIN.

4.6 Manejo de Claves del PIN

El control de clave es el proceso de crear, distribuir, mantener, guardar y destruir las claves criptográficas, incluyendo las políticas y los procedimientos asociados usados por las entidades de procesamiento.

Todos los Adquirientes y sus agentes que realizan el procesamiento de Transacciones con PIN deben acatar los requisitos de seguridad para el manejo de claves y de PIN especificados en *Payment Card Industry PIN Security Requirements*.

Además, todos los Adquirientes y sus agentes deben cumplir con las Normas de encriptado de PIN que se muestran a continuación:

1. Efectuar todo el encriptado, traducción y desencriptado de los PIN para la red utilizando encriptado de hardware.
2. No efectuar el encriptado, traducción o desencriptado del PIN bajo las rutinas del software de la Norma de Encriptado de Datos Triple (DES).
3. Usar al algoritmo de DES Triple para ejecutar todo el encriptado.

Todos los Emisores y sus agentes que efectúan el procesamiento del PIN deben consultar las *Issuer PIN Security Guidelines* referente a todos los aspectos del manejo de claves de PIN y de PIN del Emisor, que incluyen la selección, transmisión, almacenamiento, guía de uso del PIN y cambio de PIN.

4.6.1 PIN Transmission Between Customer Host Systems and the Interchange System

The Interchange System and Customers exchange PIN encryption keys (PEKs) in two manners: **statically** and **dynamically**. Directly connected Customers that are processing Transactions that contain a PIN may use either static or dynamic key encryption to encipher the PIN.

MasterCard strongly recommends using dynamic PEKs. Static PEKs must be replaced as indicated in the references below.

For information about PIN key management and related services, including requirements for key change intervals and emergency keys, refer to the manuals listed in Table 4.1, which are available through the MasterCard Connect™ Publications product.

Table 4.1—PIN Key Management References

For Transaction authorization request messages routed through…	Refer to…
MasterCard Network/Dual Message System	*Authorization Manual*
MasterCard Network/Single Message System	*Single Message System Specifications*

For Transaction authorization request messages routed through…	Refer to…
MasterCard Key Management Center via the On-behalf Key Management (OBKM) Interface	*On-behalf Key Management (OBKM) Procedures* and *On-behalf Key Management (OBKM) Interface Specifications*

4.6.2 On-behalf Key Management

MasterCard offers the On-behalf Key Management (OBKM) service to Europe Region Customers as a means to ensure the secure transfer of Customer cryptographic keys to the MasterCard Key Management Center. OBKM services offer Customers three key exchange options:

- **One-Level Key Hierarchy**—Customers deliver their cryptographic keys in three clear text components to three MasterCard Europe security officers. The security officers then load the key components into the Key Management Center.
- **Two-Level Key Hierarchy**—The Key Management Center generates and delivers transport keys to Customers in three separate clear text components. Customers use the transport keys to protect and send their cryptographic keys to Key Management Services in Waterloo, Belgium. Key Management Services then loads the Customer keys into the Key Management Center.
- **Three-Level Key Hierarchy**—The Key Management Center uses public key techniques to deliver transport keys to Customers in three separate clear text components. Customers use the transport keys to protect and send their cryptographic keys to Key Management Services in Waterloo, Belgium. Key Management Services then loads the Customer keys into the Key Management Center.

MasterCard recommends that Customers use the Two-Level or Three-Level Key Hierarchy, both of which use transport keys to establish a secure channel between the Customer and the Key Management Center.

MasterCard has developed a Cryptography Self Test Tool (CSTT) to assist Customers in meeting OBKM interface requirements. Customers must use the CSTT before exchanging keys with Key Management Services using the Two-Level and Three-Level Hierarchies.

Customers must register to participate in the OBKM service. For more information, contact key_management@mastercard.com or refer to the *On-behalf Key Management (OBKM) Procedures* and *On-behalf Key Management (OBKM) Interface Specifications*, available via the MasterCard Connect™ Publications product.

4.7 PIN at the POI for MasterCard Magnetic Stripe Transactions

MasterCard may authorize the use of a PIN for MasterCard magnetic stripe Transactions at selected Merchant types, POS Terminal types, or Merchant locations in specific countries. MasterCard requires the use of a PIN at CAT 1 devices. Acquirers and Merchants that support PIN-based MasterCard magnetic stripe Transactions must provide Cardholders with the option of a signature-based Transaction, unless the Transaction occurs at a CAT 1 device or at a CAT 3 device with offline PIN capability for Chip Transactions.

MasterCard requires Merchants to provide a POS Terminal that meets specific requirements for PIN processing wherever an approved implementation takes place. When applicable, each Transaction must be initiated with a Card in conjunction with the PIN entered by the Cardholder at the terminal. The Acquirer must be able to transmit the PIN in the Authorization Request/0100 message in compliance with all applicable PIN security Standards.

Acquirers and Merchants must not require a Cardholder to disclose his or her PIN, other than by private entry into a secure PIN entry device (PED) as described in section 4.9 of this manual.

Acquirers must control Terminals equipped with PIN pads. If a terminal is capable of prompting for the PIN, the Acquirer must include the PIN and full magnetic stripe-read data in the Authorization Request/0100 message.

MasterCard will validate the PIN when processing for Issuers that provide the necessary keys to MasterCard pursuant to these Standards. All other POI Transactions containing PIN data will be declined in Stand-In processing.

4.8 Normas de Seguridad de la Terminal

El Adquiriente debe asegurarse de que cada Terminal:

1. Tenga un lector de banda magnética con capacidad de leer los datos de la Pista 2 y transmitirlos al Emisor para su autorización;
2. Permita al Tarjetahabiente ingresar los datos del PIN de forma privada;
3. Evite que se inicie una nueva Transacción antes de que se haya completado la Transacción anterior; y
4. Valide la autenticidad de la Tarjeta o Dispositivo de Acceso.

Para las Transacciones de banda magnética, el Adquiriente debe efectuar las siguientes verificaciones (en la Terminal o en el sistema de la computadora principal del Adquiriente) antes de enviar la solicitud de autorización:

1. **Verificación de Redundancia Longitudinal (LRC)**—La banda magnética se debe leer sin error de LRC.
2. **Formato de la Pista**—El formato de la pista debe cumplir con las especificaciones en el Apéndice A.

Con relación a las funciones electrónicas que efectúa una Terminal, aplican los siguientes requisitos:

1. No se debe rechazar una Transacción debido a la validación del número de identificación bancaria (BIN)/Número de identificación del emisor (IIN).
2. No se debe rechazar una Transacción como resultado de ediciones o validaciones efectuadas en la longitud del número de cuenta primario (PAN), fecha de vencimiento, código de servicio, datos discrecionales o en los datos del dígito de verificación del Dispositivo de Acceso.
3. Las pruebas o ediciones en la Pista 1 no deben efectuarse con el propósito de descalificar a una Tarjeta para su elegibilidad al procesamiento del Sistema de Intercambio.

4.9 Hybrid Terminal Security Standards

The Acquirer must ensure that a Hybrid Terminal complies with all of the following Standards:

- Each Hybrid POS Terminal that reads and processes EMV-compliant payment applications must read and process EMV-compliant MasterCard and Maestro Payment Applications.
- Each Hybrid ATM and Hybrid PIN-based In-Branch Terminal that reads and processes EMV-compliant payment applications must read and process EMV-compliant MasterCard, Maestro, and Cirrus Payment Applications.
- Each Hybrid Terminal must perform a Chip Transaction when a Chip Card or Access Device is presented in compliance with all applicable Standards, including those Standards set forth in the *M/Chip Requirements* manual.
- Each offline-capable Hybrid POS Terminal must support offline Static Data Authentication (SDA) and offline Dynamic Data Authentication (DDA) as Card authentication methods (CAMs). Each offline-capable Hybrid POS Terminal certified by MasterCard on or after 1 January 2011 also must support offline Combined Data Authentication (CDA) as a CAM.
- Except in the United States Region, each offline-capable Hybrid POS Terminal certified by MasterCard on or after 1 January 2011 must support offline PIN processing as a Cardholder verification method (CVM). In Taiwan, this requirement applies to Hybrid POS Terminals certified by MasterCard on or after 1 January 2013.
- In the United States Region, each Hybrid POS Terminal that supports PIN must support both online PIN and offline PIN processing.
- Each Hybrid POS Terminal that supports offline PIN processing must support both clear text and encrypted PIN options.

4.10 PIN Entry Device Standards

A PED on an ATM Terminal, PIN-based In-Branch Terminal, or POS Terminal must have a numeric keyboard to enable the entry of PINs, with an 'enter key' function to indicate the completion of entry of a variable length PIN.

In all Regions except the Canada and United States Regions, a PED must accept PINs having four to six numeric characters. In the Canada and U.S. Regions, a PED must support PINs of up to 12 alphanumeric characters. It is recommended that all PEDs support the input of PINs in letter-number combinations as follows:

1	Q, Z	6	M, N, O
2	A, B, C	7	P, R, S
3	D, E, F	8	T, U, V
4	G, H, I	9	W, X, Y
5	J, K, L		

An Acquirer must ensure that all PEDs that are part of POS Terminals meet the following Payment Card Industry (PCI) requirements:

1. All PEDs must be compliant with the *Payment Card Industry PIN Security Requirements* manual.
2. All newly installed, replaced, or refurbished PEDs must be compliant with the PCI POS PED Security Requirements and Evaluation Program.
3. All PEDs must be in compliance with the PCI POS PED Security Requirements and Evaluation Program or appear on the MasterCard list of approved devices.

As a requirement for PED testing under the PCI POS PED Security Requirements and Evaluation Program, the PED vendor must complete the forms in the *Payment Card Industry POS PIN Entry Device Security Requirements* manual, along with the *Payment Card Industry POS PIN Entry Device Evaluation Vendor Questionnaire*. The vendor must submit all forms together with the proper paperwork, including the required PED samples, to the evaluation laboratory.

If a Customer or MasterCard questions a PED with respect to physical security attributes (those that deter a physical attack on the device) or logical security attributes (functional capabilities that preclude, among other things, the output of a clear text PIN or a cryptographic key), MasterCard has the right to effect an independent evaluation performed at the manufacturer's expense.

MasterCard will conduct periodic security reviews with selected Acquirers and Merchants. These reviews will ensure compliance with MasterCard security requirements and generally accepted best practices.

ADVERTENCIA:

The physical security of the PED depends on its penetration characteristics. Virtually any physical barrier may be defeated with sufficient effort.

For secure transmission of the PIN from the PED to the Issuer host system, the PED must encrypt the PIN using the approved algorithm(s) for PIN encipherment listed in ISO 9564-2 and the appropriate PIN block format as provided in ISO 9564-1.

If the PIN pad and the secure component of the PED are not integrated into a single tamper-evident device, then for secure transmission of the PIN from the PIN pad to the secure component, the PIN pad must encrypt the PIN using the approved algorithm(s) for PIN encipherment listed in ISO 9564-2.

4.11 Normas de Seguridad de las Terminales de POS Inalámbricas y de las Terminales de POS con capacidad de IP de Internet/Independiente

MasterCard ha establecido requisitos de seguridad para el encriptado de datos confidenciales de las Terminales de POS. Estos requisitos aplican a las Terminales de POS que utilizan tecnologías inalámbricas de amplio alcance, tales como el servicio general de radio por paquete (GPRS) y el acceso múltiple por división de código (CDMA), para comunicarse a las computadoras principales y a las terminales conectadas a los IP independientes que se vinculan mediante Internet.

Todas las Terminales de POS inalámbricas y las Terminales de POS con capacidad de IP/Internet deben apoyar el encriptado de los datos de la Transacción y del Tarjetahabiente entre la Terminal de POS y el sistema del servidor con el cual se comunican, utilizando los algoritmos de encriptado aprobados por MasterCard.

Si las Terminales de POS con capacidad de IP/Internet utilizadas son susceptibles a ataques desde redes públicas, los Adquirientes deben asegurarse de que sean aprobadas por el Programa de Pruebas de Seguridad de la Terminal de POS (PTS) de IP de MasterCard.

Las Terminales de POS con capacidad de IP/Internet pueden presentarse para la evaluación de seguridad en los laboratorios reconocidos por el Programa de Pruebas de PTS de IP de MasterCard para su posterior aprobación.

Todos los Adquirientes que utilicen Terminales de POS con capacidad de Internet/IP o Terminales de POS inalámbricas deben tomar como referencia los documentos de seguridad requeridos que figuran a continuación:

- *POS Terminal Security Program—Program Manual [Programa de Seguridad de la Terminal de POS—Manual del Programa]*
- *POS Terminal Security Program—Security Requirements [Programa de Seguridad de la Terminal de POS—Requisitos de Seguridad]*
- *POS Terminal Security Program—Derived Test Requirements [Programa de Seguridad de la Terminal de POS—Requisitos de Pruebas de Derivación]*
- *POS Terminal Security Program—Vendor Questionnaire [Programa de Seguridad de la Terminal de POS—Cuestionario del Proveedor]*
- *Payment Card Industry Data Security Standard [Norma de Seguridad de Datos de la Industria de Tarjetas de Pago]* (elaborada por el Consejo de Normas de Seguridad de la PCI)
- Cualquier otro documento de seguridad relacionado que MasterCard puede publicar periódicamente.

4.12 Terminales de POS que Usan la Tecnología de Captura de Firma Electrónica (ESCT)

Un Adquiriente que utiliza Terminales de POS que usan la Tecnología de Captura de Firma Electrónica (ESCT) debe asegurarse de lo siguiente:

- Que la seguridad y los controles adecuados del procesamiento electrónico de datos (EDP) estén implementados, para que las firmas digitalizadas se puedan volver a crear con base en una Transacción específica. El Adquiriente podría volver a crear la firma capturada de una Transacción específica solamente en respuesta a una solicitud de recuperación de esa Transacción.
- Que existan los controles adecuados para los empleados con acceso autorizado a las firmas digitalizadas que se mantienen en las computadoras principales del Adquiriente o del Comercio. Solamente los empleados y agentes con la "necesidad de saber" deben tener acceso a las firmas electrónicamente capturadas y almacenadas.
- Que no se pueda tener acceso a las firmas digitales ni usar las mismas de forma que sea contraria a las Normas.

MasterCard se reserva el derecho de auditar a los Clientes para asegurar el acatamiento de estos requisitos y puede prohibir el uso de la ESCT si descubre controles inadecuados.

4.13 Autenticación del Componente

Todos los componentes que participan activamente en el Sistema de Intercambio deben autenticarse mutuamente por medio de procedimientos criptográficos; ya sea explícitamente por medio de un protocolo de autenticación específico o implícitamente por medio de la ejecución correcta de un servicio criptográfico que posee información secreta (por ejemplo, la clave compartida o la identificación del registro).

Un componente participa activamente en el Sistema de Intercambio si, debido a su posición en el sistema, puede evaluar, modificar o procesar información relacionada con la seguridad.

4.14 Normas de Migración a DES Triple

La Norma de Encriptado de Datos Triple (DES), longitud de clave doble mínima (de aquí en adelante denominada "DES Triple"), se debe implementar de la siguiente manera:

- Todos los PED instalados recientemente, incluyendo el reemplazo y renovación de los PED que son parte de las Terminales de POS, deben tener capacidad para DES Triple. Este requisito aplica a las Terminales de POS de propiedad de los Clientes y No Clientes.
- Todas los sistemas de computadoras principales de los Clientes y de los procesadores deben apoyar la DES Triple.
- Se recomienda enfáticamente que todos los PED que son parte de las Terminales de POS acaten la DES Triple y tengan capacidad de chip.

- Todos los PED que son parte de las Terminales de ATM deben acatar la DES Triple.
- Todas las Transacciones basadas en el PIN distribuidas al Sistema de Intercambio deben acatar la DES Triple.

MasterCard reconoce que los Clientes pueden optar por usar otros métodos de encriptado de claves públicas entre sus Terminales de POS o ATM y sus computadoras principales. En dichos casos, MasterCard debe aprobar el método alternativo elegido antes de su implementación y uso.

La aprobación dependerá, en parte, de si MasterCard considera que ese método alternativo es tan o más seguro que la DES Triple. **Antes de iniciar la implementación, se requiere aprobación**. Todas las Transacciones distribuidas al Sistema de Intercambio deben acatar la DES Triple.

Capítulo 5 Normas de Recuperación y Devolución de Tarjetas

Este capítulo puede ser de interés particular para los Clientes que emiten Tarjetas de MasterCard®. Incluye pautas para el personal a cargo de la retención y devolución de Tarjetas, de informar las Tarjetas extraviadas y robadas y de las investigaciones criminales y de falsificación.

5.1 Recuperación y Devolución de Tarjetas

Las siguientes secciones tratan sobre responsabilidades del Cliente relacionadas con la retención y devolución de Tarjetas, las recompensas por Captura de tarjetas, informes de Tarjetas perdidas y robadas e investigaciones criminales y de falsificación.

5.1.1 Retención de Tarjetas por parte de los Comercios

Los Adquirientes y Comercios deberán hacer sus mejores esfuerzos para recuperar una Tarjeta por medios razonables y pacíficos si:

- El Emisor aconseja al Adquiriente o Comercio a recuperar la Tarjeta en respuesta a una solicitud de autorización.
- El número de cuenta está incluido en el archivo del Electronic Warning Bulletin o en la *Notificación de Advertencia* regional vigente.

Después de recuperar una Tarjeta, el Adquiriente o Comercio que la recupere deberá notificar a su centro de autorización o a su Adquiriente y recibir las instrucciones para devolver la Tarjeta. Si la Tarjeta se envía por correo, el Adquiriente o Comercio que la recupera, debe cortar primero la Tarjeta a la mitad a través de la banda magnética.

No se permite la captura de la Tarjeta Maestro en una Terminal de Punto de Venta (POS) con respecto a las Transacciones Entre Regiones o a las Transacciones Dentro de la Región que ocurran en las Regiones de Asia/Pacífico, América Latina y el Caribe o de Estados Unidos.

5.1.1.1 Returning Recovered Cards

The Acquirer must follow these procedures when returning a recovered Card to the Issuer:

1. If the Merchant has not already done so, the Acquirer must render the Card unusable by cutting it in half vertically through the magnetic stripe.
2. The Acquirer must forward the recovered Card to the Issuer within five calendar days of receiving the Card along with the first copy (white) of the Interchange Card Recovery Form (ICA-6). The additional copies are file copies for the Acquirer's records. Unless otherwise noted in the "Other Information" section of the Member Information tool, a recovered Card must be returned to the Security Contact of the Issuer.

NOTA: A sample of the Interchange Card Recovery Form (ICA-6) appears in the Business Forms section of MasterCard Connect™.

A Merchant may return a Card inadvertently left at the Merchant location if the Cardholder claims the Card before the end of the next business day and presents positive identification. With respect to unclaimed Cards, a Merchant must follow the Acquirer's requirements as set forth in the Merchant Agreement.

5.1.1.2 Cómo Devolver Tarjetas Falsificadas

El Adquiriente o Comercio deberá devolver las Tarjetas falsificadas al Emisor siguiendo las instrucciones proporcionadas por su centro de autorización. La información a continuación identifica a un Emisor:

- El número de identificación bancario (BIN) de MasterCard del Emisor presente en el Area de Información de la Cuenta.
- La Identificación del Miembro impresa en el área de Identificación de la Fuente de Tarjetas en el reverso de la Tarjeta.

Ante la ausencia de una Identificación del Miembro o BIN, el Emisor puede identificarse por otros medios, incluyendo el nombre del banco impreso en el frente o reverso de la Tarjeta o la banda magnética. Si el Emisor sigue sin ser identificado, devuelva la Tarjeta al Vicepresidente del Departamento de Servicios de Seguridad y Riesgos de MasterCard.

NOTA: El método de identificación del Emisor descrito aplica únicamente a la devolución de una Tarjeta falsificada, no para determinar el Cliente responsable por las pérdidas por falsificaciones relacionadas con estas Tarjetas. Para más información, consulte el capítulo 6—Normas de Control de Pérdidas por Fraude de este manual.

5.1.1.3 Responsabilidad por Pérdida, Costos y Daños

Ni MasterCard ni ninguno de sus Clientes será responsable por las pérdidas, costos u otros daños por reclamaciones declaradas contra ellos por un Emisor por las acciones solicitadas por ese Emisor de incluir una cuenta o un listado de un Grupo o Serie en el archivo del Electronic Warning Bulletin o en la *Notificación de Advertencia* regional correspondiente. Consulte el *Account Management System User Manual* para obtener más información sobre los procedimientos para listar las cuentas.

Si un Adquiriente utiliza estos procedimientos por equivocación sin las pautas del Emisor y autoriza al Comercio a recuperar una Tarjeta no incluida en el archivo del Electronic Warning Bulletin o en la *Notificación de Advertencia* regional correspondiente, ni MasterCard ni sus Clientes serán responsables de la pérdida, los costos u otros daños si se realiza una reclamación contra ellos.

Ningún Cliente es responsable bajo esta sección de cualquier reclamación a menos que el Cliente tenga:

- Notificación por escrito de que se ha presentado una reclamación, dentro de un plazo de 120 días a partir de la fecha en que se haya presentado la reclamación, y
- Oportunidad adecuada de controlar la defensa o liquidación de cualquier litigio relacionado con la reclamación.

5.1.2 Retención de Tarjetas en ATM

La retención de la tarjeta deberá tener lugar únicamente por orden del Emisor. Las tarjetas retenidas debido a un problema de funcionamiento de la Terminal de ATM o por un error del Tarjetahabiente, sobre el cual el dueño de la Terminal de ATM no tiene control, serán las únicas excepciones permitidas. Si un Adquiriente de ATM no puede determinar en dos días

hábiles si una Tarjeta fue retenida debido a un mal funcionamiento de la máquina, a un error del Tarjetahabiente, o por una orden enviada por el Emisor, la Tarjeta será considerada como una Tarjeta retenida a pedido del Emisor.

Un Adquiriente de la Terminal de ATM que como un Emisor envía órdenes de retención de Tarjeta debe aceptar esas órdenes enviadas por otros Emisores en todos sus ATM que tienen capacidad para retener Tarjetas.

En la Región de Europa, el Adquiriente de cualquier Terminal de ATM con capacidad para retener la Tarjeta debe aceptar las órdenes de retención de Tarjeta enviadas por cualquier Emisor.

Los mensajes de acatamiento deben indicar, bajo el mejor conocimiento del Adquiriente, la acción tomada por el ATM por cada solicitud de retener la Tarjeta.

5.1.2.1 Cómo Manejar las Tarjetas Retenidas en ATM

Un Adquiriente de la Terminal de ATM debe manejar las Tarjetas retenidas de acuerdo con los siguientes requisitos:

1. Todas las tarjetas retenidas de MasterCard deberán registrarse bajo un control doble inmediatamente después de sacarlas de los ATM. Con respecto a las Tarjetas de Maestro y Maestro retenidas, es responsabilidad del Adquiriente establecer los procedimientos adecuados para documentar la retención de una Tarjeta.
2. Destruir las Tarjetas retenidas cortándolas por la mitad verticalmente a través de la banda magnética, si la Tarjeta es retenida por orden del Emisor o si los procedimientos de un Adquiriente no incluyen la devolución de las Tarjetas retenidas a los Tarjetahabientes. Una Tarjeta Maestro emitida fuera de la Región de Europa y retenida por una Terminal de ATM ubicada en la Región de Europa debe ser destruida y eliminada.

Cuando una tarjeta retenida parece ser fraudulenta (por ejemplo, una tarjeta de cartón o una tarjeta de plástico blanca), el Adquiriente puede (a su elección) retener, conservar y entregar dicha tarjeta a las autoridades competentes.

5.1.2.2 Cómo Devolver las Tarjetas Retenidas en ATM a los Tarjetahabientes

Las tarjetas retenidas a solicitud de un Emisor nunca se deberán devolver al Tarjetahabiente sin permiso del Emisor. Sin embargo, las Tarjetas retenidas erróneamente por el Adquiriente debido a un mal funcionamiento de la máquina, falla del sistema o un error del Tarjetahabiente podrán ser retenidas en la ubicación del ATM, en un lugar seguro, durante dos días hábiles posteriores a la retención y entregadas al Tarjetahabiente luego de todo lo siguiente:

1. El Adquiriente verifica el archivo del Electronic Warning Bulletin o el *Aviso de Advertencia* regional correspondiente (requerido solamente por las Tarjetas MasterCard®).
2. El Tarjetahabiente presenta identificación razonable (por ejemplo, licencia de conducir vigente, pasaporte o identificación similar con una foto o datos descriptivos y una firma que se compara con la firma en la Tarjeta retenida, si corresponde).
3. El Tarjetahabiente firma un registro o recibo de disposición, o el Adquiriente de otro modo conserva un registro de la medida tomada.

El Adquiriente debe notificar entonces al Emisor y explicar que la Tarjeta fue retenida, las circunstancias de la retención y que la Tarjeta se devolvió al Tarjetahabiente.

Si el Tarjetahabiente no regresa para reclamar la Tarjeta antes del final del segundo día hábil siguiente a la retención de la Tarjeta, se deberá destruir la banda magnética de la Tarjeta.

Un Adquiriente no tendrá ninguna responsabilidad por las Transacciones fraudulentas o sin autorización iniciadas con una Tarjeta que haya devuelto dicho Adquiriente al Tarjetahabiente después de la retención de la Tarjeta en una Terminal de ATM, siempre y cuando dicho Adquiriente haya acatado los requisitos descritos en esta sección.

5.1.2.3 Cargos por Retención y Devolución de Tarjetas en ATM

El Adquiriente no debe cobrar al Emisor ningún cargo por la retención en ATM o devolución de una Tarjeta.

5.1.3 Pago de Recompensas

El Adquiriente puede, a su elección, pagar al Comercio o al cajero de la institución financiera una recompensa por retener una Tarjeta de acuerdo con las prácticas locales. La recompensa deberá pagarse a la persona que retenga la Tarjeta.

5.1.3.1 Normas de los Pagos de Recompensas

El Adquiriente deberá seguir estas Normas al pagar una recompensa:

1. Pagar no menos de USD 50 al Comercio que recupera una Tarjeta incluida en un archivo del Electronic Warning Bulletin o en la *Notificación de Advertencia* y no menos de EUR 50 al Comercio que recupera una Tarjeta incluida en la Región D en el archivo del Electronic Warning Bulletin.
2. Pagar USD 100 (EUR 100 cuando el Comercio está en la región de Europa y la Tarjeta válida fue emitida en la Región de Europa) al Comercio, **si** un Comercio inicia una llamada de autorización debido a una Transacción sospechosa o captura una Tarjeta no incluida en el archivo del Electronic Warning Bulletin o en la *Notificación de Advertencia*.
3. Pagar una recompensa a un cajero de una institución financiera por la captura de otra Tarjeta de Cliente, si es costumbre del Adquiriente pagarles a sus cajeros recompensas por recuperar sus propias Tarjetas. El monto de la recompensa debe ser el mismo monto pagado por la captura de las Tarjetas del Adquiriente dentro de los límites establecidos en la sección 5.1.3.2.
4. Cobrarle al Emisor por el reembolso de la recompensa pagada al enviar cada Tarjeta retenida por el Comercio o por un cajero de una institución financiera. El mensaje de Cobro de Cargo/1740 con un código de motivo de mensaje de Producto Integrado (IPM) [Elemento de Datos 25] igual a 7601 liquidará la recompensa.

5.1.3.2 Montos de Recompensas

El Adquiriente deberá seguir estas pautas para determinar los montos de recompensa.

Tabla 5.1—Determinaciones del Monto

SI la captura...	ENTONCES pague este monto...
Fue resultado de una llamada telefónica por concepto de "Comercio Sospecha Fraude"	USD 100 (EUR 100 cuando el Comercio está en la Región de Europa y la Tarjeta válida fue emitida en la Región de Europa)
No fue resultado de una llamada telefónica por "Comercio Sospechosa Fraude"	USD 50 (EUR 50 en la Región de Europa)
Lleva a la retención de Tarjetas adicionales	USD 50/EUR 50 por cada Tarjeta retenida, con un total máximo de USD 250/EUR 250 por cualquier incidente

La condición de que la persona que retiene la Tarjeta recuperada recibe una recompensa, según se estipula en la sección 5.1.3, no impide que los Clientes hagan convenios aceptados mutuamente entre ellos relacionados con las recompensas.

El Cliente que recupera la tarjeta puede cobrar un cargo administrativo de USD 15 por los gastos incurridos al procesar la Tarjeta retenida. Un Cliente que recupera la Tarjeta en la Región de Europa puede cobrar un cargo administrativo de EUR 15 por dichos gastos. El Cliente que retiene la Tarjeta puede agregar este cargo al monto del reembolso de la recompensa o cobrar el cargo de forma independiente, usando el mensaje de Cobro de Cargo/1740.

5.1.3.3 Reembolso de Recompensas

Las siguientes especificaciones se aplican al reembolso de recompensas:

- Al enviar la Tarjeta al Emisor, el Adquiriente obtendrá un reembolso por la recompensa pagada y el cargo de USD 15 o EUR 15 al procesar el mensaje de Cobro de Cargo/1740.
- Si un Cliente devuelve una Tarjeta a un Emisor y no se paga una recompensa, el Cliente que recupera la Tarjeta puede, a su criterio, cobrar un cargo de USD 15 o EUR 15 al procesar el registro de mensaje de Cobro de Cargo/1740.
- Al recibir el Interchange Card Recovery Form [Formulario de Recuperación de Tarjeta de Intercambio] (ICA-6), el Emisor deberá cotejarlo con el registro del mensaje de Cobro de Cargo/1740 basándose en la comparación del número de Identificación del Miembro del Adquiriente, el número de cuenta y la fecha de recuperación.
- Si un Cliente exento tiene un pago de recompensa electrónico procesado, la compensación recibe el registro mediante un comprobante de información. La Transacción será parte del Sistema de Liquidación Neta para fines de liquidación.

5.1.3.4 Contracargos de los Pagos de Recompensas

Se podrá contracargar un documento de reembolso por recompensa únicamente cuando se le cargue a un Cliente incorrecto. El vicepresidente principal del Departamento de Servicios de Seguridad y Riesgos resolverá cualquier disputa relacionada con el reembolso de una recompensa.

5.1.4 Cómo Informar sobre el Uso Fraudulento de Tarjetas

Un Emisor debe presentar mensualmente todas las Transacciones fraudulentas sobre sus Cuentas al Sistema para Evitar el Fraude con Eficacia (SAFE), según se describe en el Capítulo 12. Para el beneficio de todos los Clientes, MasterCard analiza los datos y produce estadísticas relacionadas con el uso fraudulento de las cuentas de MasterCard y todos los contracargos que se originan de Transacciones que usan cuentas con un estado de fraude.

El Emisor deberá informar las Transacciones fraudulentas aunque haya recuperado las pérdidas por medio de contracargos, casos de acatamiento, restitución, seguro o por cualquier otro medio.

Un Adquiriente que recibe una Transacción que no puede ser identificada con un BIN o número de Identificación de Miembro de MasterCard es responsable de esa Transacción. Si se determina que la Transacción es una Transacción fraudulenta o falsificada, el Adquiriente debe informar, por escrito, al Departamento de Servicios de Seguridad y Riesgo de dicho incidente. Esta notificación debe incluir toda la información obligatoria según se describe en el Capítulo 7 de la *SAFE Products User Guide*.

5.1.5 Reporting Lost and Stolen Cards

A Customer, or a Third Party Processor (TPP) acting as the Customer's or its Sponsor's authorized agent, that receives a lost or stolen Card report must promptly notify the Issuer of the report. The Customer should send the notice via phone and direct it to the Issuer's Security Contact identified in the Member Information tool available on MasterCard Connect™. If an Issuer requests to receive such notice by another method, then the Customer should comply with the Issuer's request.

The notice must include all relevant available information, such as:

- Member ID of the institution sending the notice
- Issuer's name
- Cardholder's account number
- Cardholder's name and address
- Phone number and an address where the Cardholder can be reached

If the Customer cannot immediately reach the Issuer by phone, the Customer must make another attempt at the first opportunity during the Issuer's normal business hours. Issuers must accept all collect calls placed to report a lost or stolen Card.

NOTA: The Issuer will be responsible for the reasonable costs of transmitting the notice.

For international notifications only, in lieu of a phone message, a telex or cable message is acceptable. The Issuer is responsible for the reasonable costs of transmitting the notice and must accept collect calls. The notice should include the same information previously mentioned. In addition, the Customer making the report should follow the international notice with a written confirmation within three business days.

The Customer that receives and transmits the report may submit to the Issuer an IPM Fee Collection/1740 message with message reason code 7600 to collect the USD 15 lost or stolen Card report fee in addition to any transmission costs that it may incur.

If the account number is unknown, the reporting Customer still may use the IPM Fee Collection/1740 message by zero-filling the Account Number field and by providing the Cardholder's name and address, and the Issuer's name or service mark, in the Data Text field.

NOTA: Issuers may direct Cardholders to the MasterCard Assistance Center at 1-800-307-7309.

5.1.5.1 Informes que Recibe MasterCard

MasterCard ayudará a sus Clientes recibiendo los informes de Tarjetas extraviadas o robadas y (a opción de cada Cliente) tomará el informe y notificará rápidamente al Emisor o, si el informe es por teléfono, remitirá la llamada al Emisor (cuando esta capacidad esté disponible). Solamente si el Emisor lo solicita, MasterCard actualizará con prontitud el archivo negativo de autorización usado para el procesamiento Stand-In.

MasterCard puede cobrar al Emisor USD 15 por informe además de costos de transmisión en que pudiera incurrir por recibir y transmitir el informe.

5.2 Investigaciones Delictivas y sobre Falsificaciones

A solicitud, cada Cliente debe proporcionar a otros Clientes una ayuda razonable de investigación en la zona geográfica cubierta por su propio plan de Tarjetas y tendrá derecho a un reembolso del Cliente que solicita por los gastos reales y a un cargo por hora de investigación, según lo establezca MasterCard periódicamente. Los procedimientos para solicitar dicha asistencia aparecen a continuación.

5.2.1 Cómo Iniciar una Investigación

Para iniciar una investigación, el Cliente que solicita debe seguir los siguientes pasos:

1. Completar la parte A del Formulario de Solicitud e Informe de Investigación (ICA-7A)
2. Enviar las copias correspondientes del formulario de cinco partes a:
   - El Contacto de Seguridad del Cliente que realiza la investigación, y
   - El Departamento de Servicios de Seguridad y Riesgo a la dirección proporcionada en el Apéndice C.

En el caso de una emergencia, el Cliente puede iniciar una investigación telefónica o por télex. Sin embargo, la solicitud debe contener toda la información pertinente en el Investigation Request and Report Form [Formulario de Solicitud e Informe de Investigación]. El Cliente

deberá remitir las copias correspondientes del formulario dentro de un plazo de 36 horas después de hacer la solicitud por teléfono o télex.

5.2.2 Cómo Proporcionar un Informe de Progreso

El Cliente investigador debe acusar recibo del Formulario Investigation Request and Report Form [Formulario de Solicitud e Informe de Investigación] dentro de un plazo de tres días hábiles. Dentro de 15 días hábiles del recibo del Formulario de Solicitud e Informe de Investigación, el Cliente que investiga deberá proporcionar un informe de progreso de los resultados de la investigación. Si no se puede completar la investigación dentro de los 15 días, el Cliente que investiga deberá completar la investigación tan pronto como sea posible. El Cliente investigador deberá utilizar el mismo Investigation Request and Report Form [Formulario de Solicitud e Informe de Investigación] para resumir los resultados de una investigación.

El formulario sirve también como factura que se envía al Cliente solicitante por las horas de personal y gastos relacionados con la investigación. El Cliente que lleva a cabo la investigación deberá llenar la parte B del formulario y distribuir las copias de acuerdo con las instrucciones en el Investigation Request and Report Form [Formulario de Solicitud e Informe de Investigación].

5.2.3 Cómo Solicitar el Arresto y Procesamiento en los Tribunales Penales

Cuando un Cliente solicita que otro Cliente ocasione el arresto y procesamiento penal posterior de un individuo por el uso indebido de una Tarjeta, el Cliente que solicita debe proporcionar todos los testigos necesarios en los diferentes procedimientos penales.

5.2.4 Fees and Reimbursement of Expenses

The investigating Customer may collect from the requesting Customer USD 50 for each half hour of investigative work performed. The Investigation Request and Report Form (ICA-7A) details all costs and expenses incurred by investigative personnel on behalf of the requesting Customer, or the amount specifically authorized by the requesting Customer to be used for investigation expenses.

NOTA: A sample of the Investigation Request and Report Form (ICA-7A) appears in the Business Forms section of MasterCard Connect™.

When a Customer requests that another Customer cause the arrest and subsequent criminal prosecution of an individual for misuse of a Card, the requesting Customer must pay all related expenses at the various criminal proceedings.

MasterCard can authorize the expenditure of any funds necessary to conduct a counterfeit or major criminal investigation, including reimbursement of a Customer's expenses in any particular case that caused a hardship to that Customer.

To settle investigation fees and expenses, Customers should use the IPM Fee Collection/1740 message with message reason code 7610.

5.2.5 Investigación de Casos de Falsificaciones y Delitos Importantes

Los diferentes vicepresidentes regionales de MasterCard del Departamento de Servicios de Seguridad y Riesgo tienen la autoridad para manejar la investigación de un caso de falsificación o penal. Cuando se les solicite, los Clientes deberán proporcionar la ayuda necesaria al vicepresidente regional.

Capítulo 6 Normas de Control de Pérdidas por Fraude

Este capítulo puede ser de interés particular para el personal responsable de los programas de control de pérdidas por fraude, reembolsos y procedimientos de pérdidas por falsificaciones y de las obligaciones del Adquiriente por las falsificaciones.

6.1 Customer Responsibility for Fraud Loss Control

A Customer must establish adequate fraud loss controls for each of its issuing and acquiring Programs and use them actively and effectively. A Digital Activity Customer must establish adequate fraud loss controls for each of its Digital Activity Programs and use them actively and effectively.

An Acquirer must transmit full magnetic stripe or chip data for all Point-of-Interaction (POI) Card-read Transactions.

An Issuer must, at a minimum, incorporate the Card security features described in Chapter 3 of this manual and the *Card Design Standards*, and comply with the Card production Standards described in Chapter 2 of this manual.

Sections 6.2 and 6.3 of this chapter apply to MasterCard Customers. Section 6.4 of this chapter applies to Maestro Customers.

Global Risk Management Program staff, in its sole discretion, will determine a Customer's compliance with these fraud loss control Standards and has the authority, either directly or through its designee, to perform audits and to mandate implementation and use of controls deemed necessary to achieve compliance.

6.2 Normas del Programa de Control de Pérdidas por Fraude de MasterCard

La existencia y utilización de controles significativos son medios eficaces para limitar las pérdidas totales por fraude y las pérdidas por todos los tipos de fraude. Esta sección describe los requisitos mínimos para los programas de control de pérdidas por fraude del Emisor y del Adquiriente.

6.2.1 Programas de Control de Pérdidas por Fraude del Emisor

Un programa de control de pérdidas por fraude del Emisor debe cumplir con los siguientes requisitos mínimos, y preferentemente incluirá los parámetros adicionales recomendados. El programa debe generar automáticamente informes de control de fraude diarios o alertas en tiempo real. El personal capacitado del Emisor para identificar el fraude potencial debe analizar los datos en estos informes dentro de las 24 horas.

6.2.1.1 Issuer Authorization Requirements

An Issuer must implement a rules-based authorization strategy with the following parameters:

- Decision matrix for Card validation code (CVC) 1, CVC 2, and CVC 3 validation results
- Limits on single-day and multiple-day Transaction velocity (number of Transactions)
- Limits on single-day and multiple-day monetary spending (value of Transactions)
- Limits for high-risk Card acceptor business codes (MCCs) and locations on a daily or, if necessary, more frequent basis

- Limits for particular POI entry modes (such as magnetic stripe-read, primary account number [PAN] key-entry, chip-read, Card-Not-Present [CNP])
- Limits for particular country codes
- Decision matrix for expiration date errors
- Decision matrix for Track 1 validation errors
- Decision matrix for geographic anomalies

6.2.1.2 Requisitos de Control de Fraude del Emisor

Un Emisor debe generar informes diarios o alertas en tiempo real que controlan tanto los datos de autorización como los datos de compensación, si es posible, a más tardar al día siguiente de la Transacción para los siguientes parámetros:

- Transacción única que sobrepasa cierto monto (establecido por el Emisor)
- Transacciones Múltiples que sobrepasan cierto monto (establecido por el Emisor)
- Transacciones de ingreso de PAN mediante teclado que sobrepasan cierto monto y/o volumen (establecido por el Emisor)
- Transacciones que se efectúan en locales de Comercios y MCC de alto riesgo

Un Emisor que tiene las condiciones presentes en la Tabla 6.1 debe implementar controles adicionales de pérdidas por fraude.

Tabla 6.1—Requisito Adicional de Control de Pérdidas por Fraude del Emisor

Los Emisores con ambas de las siguientes condiciones...	Deben…
• Más de dos veces el promedio global de puntos base de fraude de MasterCard • USD 200.000 o más en pérdidas anuales por fraude	Implementar programas adicionales de control de pérdidas por fraude para detectar Transacciones fraudulentas

6.2.1.3 Issuer Network Monitoring Requirements

An Issuer must use the network monitoring service provided by MasterCard for all Transactions arising from a prepaid Card Program that are processed by means of the Interchange System ("Processed Transactions"). Refer to Rule 6.10 of the *MasterCard Rules* manual for more information about prepaid Card Programs.

In the event that MasterCard detects fraudulent or potentially fraudulent activity ("suspicious activity") involving a prepaid Account, MasterCard may impose a temporary block on the affected PAN of such prepaid Account with respect to all authorization requests received for Transactions that are of the same type as the suspicious activity (for example, ATM Transactions or CNP Transactions). MasterCard will attempt to notify the Issuer of the block, and thereby enable the Issuer to implement additional controls.

6.2.1.4 Gestión de Carteras de Productos

El Emisor debe controlar sus Carteras de Cuentas para lo siguiente:

- Puntos base de fraude de la Transacción total
- Puntos base de fraude de la Transacción nacional
- Puntos base de fraude de la Transacción internacional
- Puntos base de fraude por tipo de Transacción (por ejemplo, las Transacciones de comercio electrónico [e-commerce], las Transacciones de pedidos por correo/teléfono [MO/TO] y las Transacciones con Tarjeta presente)
- Puntos base de fraude de Transacción completamente autenticada por MasterCard® *SecureCode*™

6.2.1.5 Control Adicional Recomendado al Emisor

MasterCard recomienda que los Emisores controlen de manera adicional los siguientes parámetros:

- Ataques generados por las cuentas
- Fallas en la validación del CVC 1, CVC 2 y CVC 3
- Fallas de la fecha de vencimiento
- Transacciones de número de cuenta inválido (mal asentadas)
- Transacciones en terminal activada por el tarjetahabiente (CAT)
- Transacciones de Eventos de Compromiso de los Datos de la Cuenta (ADC) o de Eventos de ADC Potencial
- Transacciones de crédito (tales como reembolsos) y reversiones de autorización del Comercio
- Fallas de validación del PIN, del token de MasterCard *SecureCode* o del Criptograma de Solicitud de Autorización (ARQC)
- Método de verificación del tarjetahabiente (CVM)
- Verificación del CVC 1 del Stand-In

6.2.1.6 Requisitos Adicionales de Control de Tarjetas Prepagadas

El Emisor debe acatar los siguientes requisitos adicionales de control para sus Programas de Tarjetas prepagadas.

Detección de Fraude

El Emisor debe desarrollar, implementar y mantener las normas formales de la Cartera de tarjetas prepagadas para controlar las situaciones de provisión de fondos. Un Emisor debe también:

- Evaluar y controlar la exposición a compromisos sin respaldo financiero; y
- Analizar regularmente las tendencias de volumen y crecimiento de Cuentas.

Control del Programa

Debe haber controles de fraude adecuados para controlar la siguiente actividad del Programa:

- Cantidad de Cuentas por Tarjetahabiente
- La cantidad de cargas efectuadas por día—Cargas que provienen de la aceptación de Tarjetas de pago en la ubicación del Punto de Venta (POS) identificado con uno de los siguientes MCC puede requerir una revisión mejorada:
  - MCC 4829 (Transferencia de Dinero—Comercio)
  - MCC 6050 (Cuasi Efectivo—Institución Financiera del Cliente)
  - MCC 6051 (Cuasi Efectivo—Comercio)
- Cantidad de cargas que provienen de la aceptación de la Tarjeta de pago efectuadas diariamente y con el tiempo (período de tiempo específico)
- Cantidad de cargas efectuadas diariamente en el mismo agente y con el tiempo
- Valor de cargas efectuadas diariamente en el mismo agente y con el tiempo
- Origen de carga—método de efectivo, Banco de Información Automatizada (ACH), transferencia de saldo de tarjeta a tarjeta o transferencia usado para la transferencia de la carga (por ejemplo, Transacción de comercio electrónico, MO/TO, o de pago recurrente)
- Reembolsos
- Patrones de recarga y retiro

Límites de la Tarjeta

Debe haber controles de fraude adecuados para controlar la siguiente actividad de la Tarjeta:

- Valores de carga inicial máximos y mínimos
- Procedimientos de recarga de tarjeta
- Cantidad máxima de cargas por Tarjeta por día
- Valor máximo en cada Tarjeta por día
- Métodos de pago aceptados para la compra, carga o recarga de la Tarjeta

6.2.1.7 Implementación de la Herramienta de Detección de Fraude

El Emisor deberá implementar una herramienta de detección de fraude que complemente de manera correcta la estrategia de fraude implementada por el Emisor. La combinación de los controles de autorización y de la herramienta de detección de fraude deberá asegurar que el Emisor controla el fraude a un nivel aceptable.

El desempeño de la herramienta de detección de fraude del Emisor deberá alcanzar al menos los requisitos de rendimiento mínimos. Se requieren los siguientes indicadores de desempeño para ayudar al Emisor a manejar una herramienta de detección de fraude eficaz. Dichos indicadores de desempeño deben incluir, entre otros:

- Tasas de detección de Fraude de la Cuenta
- Número promedio de Transacciones por caso de fraude
- Duración promedio del caso de fraude
- Pérdida promedio por caso de fraude
- Porcentaje de Transacciones de comercio electrónico fraudulentas de US$25 (o su equivalente en moneda local) o menos para la compra de Bienes Digitales informadas a través del Sistema para Evitar el Fraude con Eficacia (SAFE), comparado con el total de

Transacciones de comercio electrónico fraudulentas de US$25 (o su equivalente en moneda local) o menos informado a través del SAFE.

6.2.1.8 Estrategia de Comunicación al Tarjetahabiente

El Emisor debe implementar una estrategia de comunicación al Tarjetahabiente. Una estrategia de comunicación consiste en definir (i) los criterios para comunicarse con un Tarjetahabiente, (ii) el canal de comunicación para comunicarse con el Tarjetahabiente, y (iii) las medidas a tomar en caso de falla de comunicación con el Tarjetahabiente. Dichos canales de comunicación pueden incluir alertas del servicio de mensajes cortos (SMS), mensajes de correo electrónico, llamadas telefónicas y cartas.

6.2.2 Acquirer Fraud Loss Control Programs

An Acquirer's fraud loss control program must meet the following minimum requirements, and preferably will include the recommended additional parameters. The program must automatically generate daily fraud monitoring reports or real-time alerts. Acquirer staff trained to identify potential fraud must analyze the data in these reports within 24 hours.

To comply with the fraud loss control Standards, Acquirers also must transmit complete and unaltered data in all Card-read authorization request messages.

Additionally, Acquirers with high fraud levels must:

- Install "read and display" terminals in areas determined to be at high risk for fraud or counterfeit activity, or
- Install Hybrid POS Terminals

6.2.2.1 Requisitos de Control de Autorización del Adquiriente

Los informes diarios o las alertas en tiempo real que controlan las solicitudes de autorización del Comercio se deben generar a más tardar al día siguiente de la solicitud de autorización y deben basarse en los siguientes parámetros:

- Número de solicitudes de autorización que están por encima del margen establecido por el Adquiriente para ese Comercio
- Relación de Transacciones no de lectura de Tarjeta respecto a las de lectura de Tarjeta que está por encima del margen establecido por el Adquiriente para ese Comercio.
- Relación de ingreso de PAN mediante teclado que está por encima del margen establecido por el Adquiriente para ese Comercio.
- Solicitudes de autorización repetidas por el mismo monto o la misma cuenta de Tarjetahabiente
- Incremento del Número de solicitudes de autorización
- Volumen de Transacciones de retorno "Out of pattern" ["Fuera del patrón"]

6.2.2.2 Requisitos de Control de los Depósitos del Comercio del Adquiriente

Los informes diarios o las alertas en tiempo real que controlan los depósitos del Comercio se deben generar a más tardar al día siguiente del depósito y deben basarse en los siguientes parámetros:

- Incrementos en el volumen de depósito del Comercio
- Incremento en el tamaño del comprobante promedio del Comercio y en el número de Transacciones por depósito
- Cambio en la frecuencia de los depósitos
- Frecuencia de las Transacciones en la misma Cuenta, incluyendo las Transacciones de crédito (reembolso)
- Número inusual de créditos o volumen de crédito en dólares que exceden el nivel del volumen de ventas en dólares apropiado para la categoría del Comercio.
- Montos voluminosos de Transacciones de crédito,, significativamente más grandes que el monto promedio de las facturas de venta del Comercio
- Créditos emitidos por un Comercio posteriormente al recibo de un contracargo del Adquiriente con el mismo PAN
- Créditos emitidos por un Comercio a un PAN que no se ha usado anteriormente en el establecimiento del Comercio
- Aumentos en el volumen de contracargos del Comercio

Regla de 90 días

El Adquiriente debe comparar los depósitos diarios frente al conteo y monto de las Transacciones promedio para cada Comercio durante un período de al menos 90 días, para disminuir el efecto de las variaciones normales en el negocio de un Comercio. Para los Comercios nuevos, el Adquiriente deberá comparar el conteo y monto de la Transacción promedio para los otros Comercios dentro del mismo MCC asignado al Comercio. En el caso de que se identifique actividad de Transacción de reembolso o de crédito sospechosa, si corresponde, el Adquiriente deberá considerar la suspensión de las Transacciones pendientes de investigación posterior.

6.2.2.3 Control Adicional Recomendado al Adquiriente

MasterCard recomienda que los Adquirientes controlen además los siguientes parámetros:

- Métodos alternos
- Transacciones de crédito (tales como reembolsos) y reversiones de autorización del Comercio
- Transacciones realizadas en Comercios de alto riesgo
- Transacciones de ingreso del PAN mediante teclado que exceden la relación
- Horas o temporadas anormales
- Comercios inactivos
- Transacciones sin código de aprobación
- Tasa de transacciones rechazadas
- Elementos de datos de compensación y autorización inconsistentes para las mismas Transacciones
- Tasa de autenticación de MasterCard *SecureCode*
- Volumen de fraude por Comercio

Recomendaciones del 150 por ciento

El Comercio que aparece en los informes de control del Adquiriente deberá exceder el promedio del 150 por ciento o más, para todos los Comercios del Adquiriente como un medio para optimizar la eficacia del personal de análisis de fraude. Sin embargo, el monto sobre el promedio es a criterio del Adquiriente.

Recomendación de Control del Comercio

MasterCard recomienda a los Adquirientes utilizar una solución de control del Comercio para revisar la actividad de comercio electrónico (e-commerce) del Comercio con el fin de evitar el procesamiento de Transacciones ilegales o que perjudiquen la marca.

6.2.3 Noncompliance with Fraud Loss Control Program Standards

Following a Global Risk Management Program review, a noncompliant Customer will receive a formal written report with requirements that must be satisfied within an established period to achieve compliance with the fraud loss control Standards. For the assessments that may apply if a Customer fails to take the required actions to achieve compliance, refer to section 13.6 of this manual.

6.3 Normas de Control de Pérdidas por Fraude de Tarjeta Falsificada de MasterCard

MasterCard ayuda activamente a las autoridades del orden público en la persecución de grupos de criminales organizados e informales que se dedican al fraude con tarjetas falsificadas. Aunque MasterCard ha logrado éxitos sustanciales en esta área, incluyendo numerosas condenas de falsificadores y la incautación de sus plantas físicas, los elementos criminales organizados continúan expandiéndose y nuevos grupos surgen casi diariamente.

Además de implementar los controles de pérdidas por fraude descritos en la sección 6.2, los Clientes deben hacer un intento de buena fe para limitar las pérdidas por falsificaciones. Como mínimo, el Emisor deberá incorporar las características de seguridad de la Tarjeta descritas en el Capítulo 3 en todas la Tarjetas, y el Adquiriente debe transmitir los datos completos del chip o de la banda magnética en todas las Transacciones de POS por lectura de Tarjeta.

6.3.1 Notificación de Tarjeta Falsificada

Todos los Clientes deberán avisar a MasterCard inmediatamente al sospechar o detectar Tarjetas falsificadas.

6.3.1.1 Notification by Issuer

An Issuer must notify MasterCard immediately upon detection of a counterfeit Card bearing its bank identification number (BIN) or, in the absence of a valid BIN, its Member ID. This step must be completed by the most prompt and practical means possible, employing such methods as email, tape transmissions, phone, or telex communication.

6.3.1.2 Notification by Acquirer

An Acquirer detecting or suspecting a counterfeit Card bearing neither a valid BIN nor a valid Member ID immediately must notify its regional Security and Risk Services representative and the Issuer by phone, email, or telex communication. MasterCard will add the account number to the Account Management System.

6.3.1.3 Falla en Notificar

Si el Adquiriente o el Emisor no notifican, dentro de las 24 horas posteriores a la detección de una Tarjeta falsificada exonera a MasterCard de cualquier responsabilidad por cualquier pérdida incurrida por cualquiera de las partes que no haya proporcionado el anuncio.

6.3.2 Responsabilidad por las Pérdidas por Falsificación

Ciertas pérdidas que resultan de Transacciones por falsificación son responsabilidad ya sea del Emisor o del Adquiriente de acuerdo con las circunstancias descritas en esta sección.

6.3.2.1 Pérdidas Debidas a Fraude Interno

MasterCard no es responsable de ninguna pérdida debida a o relacionada con cualquier acto fraudulento, deshonesto o de otro modo ilícito de cualquier funcionario, director o empleado de un Cliente o del Proveedor de Servicios, agente o representante de un Cliente.

6.3.2.2 Transactions Arising from Identified Counterfeit Cards

The Issuer is responsible for any counterfeit loss resulting from or related to the use of an identified counterfeit Card. An identified counterfeit Card is determined by the BIN identified in the Transaction record or, in the absence of a BIN, by the Member ID identified in the Transaction record. The Issuer is not responsible for counterfeit losses that were or could have been charged back in accordance with the Standards or for counterfeit losses that were assumed by the Acquirer as a result of a compliance case ruling.

DEFINICIÓN:

A key-entered counterfeit Transaction occurs when the counterfeit Card is present at the POI and authorization is obtained in accordance with the Standards (but not as described for a Card-read Transaction).

DEFINICIÓN:

An imprinted counterfeit Transaction occurs when the embossed counterfeit Card is present at the POI, the Card acceptor uses an imprinter to record the Card information, and authorization is obtained, if at all, in accordance with the Standards (but not as described for a Card-read Transaction).

DEFINICIÓN:

A magnetic stripe-read counterfeit Transaction involving the use of a counterfeit Card at the POI, in which authorization is effected electronically and in accordance with the Standards, with magnetic stripe data obtained from lost or stolen Card stock is read via the Terminal and transmitted to the Issuer during the authorization process.

6.3.2.3 Transacciones que Resultan de Tarjetas Falsificadas No Identificadas

El Adquiriente es responsable de cualquier pérdida por falsificación que resulte de o esté relacionada con la aceptación del Comercio de una Tarjeta que no puede identificarse mediante un BIN o una Identificación del Miembro impresa en el registro de la Transacción.

6.3.2.4 Pérdida o Robo de Tarjetas Incompletas

Si se recupera una Tarjeta falsificada que resulta de la pérdida o del robo de Tarjetas que todavía no han sido personalizadas o que de otro modo no se completaron, el Emisor que solicitó la producción de las Tarjetas es el responsable de las pérdidas que surjan del uso de la Tarjeta falsificada. El Emisor se determina por la identificación de la fuente de la Tarjeta impresa al reverso de la Tarjeta.

6.3.3 Acquirer Counterfeit Liability Program

The Acquirer Counterfeit Liability Program is intended to combat increases in worldwide counterfeiting in the credit card industry. The Program shifts partial counterfeit loss liability to Acquirers that exceed worldwide counterfeit Standards.

Global Risk Management Program staff uses the Acquirer counterfeit volume ratio (ACVR) to evaluate all Customers' volumes of acquired counterfeit. The ACVR is a Customer's dollar volume of acquired counterfeit as a percentage of the total dollar volume acquired by that Customer.

Global Risk Management Program staff monitors the 20 Customers with the highest ACVRs on a quarterly basis. MasterCard notifies each Customer with liability of its own ACVR, the worldwide average, the reported counterfeit, and the amount of Customer liability calculated on a quarterly basis.

MasterCard uses funds obtained from Acquirers that exceed established annual thresholds to provide the following support:

- Recover the costs associated with the administration of this Program,
- Fund the development of new fraud control programs, and
- Supplement the MasterCard liability limit for the reimbursement of Issuers' counterfeit losses.

6.3.3.1 Acquirer Counterfeit Liability

An Acquirer is liable for any counterfeit volume that is above a threshold of 10 times the worldwide ACVR.

Global Risk Management Program review teams will provide a report to Acquirers whose ACVR exceeds 10 times the worldwide average with recommendations on how to reduce the volume of acquired counterfeit Transactions. If an Acquirer implements all of the programs recommended by Global Risk Management Program staff, or takes necessary action to curb counterfeit, MasterCard will review the actions taken and may adjust the cumulative liability that would otherwise be imposed by the Program.

Counterfeit experience inconsistent with the implementation of the required programs will result in further Customer Risk Reviews by MasterCard.

For more information about the Global Risk Management Program, refer to Chapter 13 of this manual.

6.3.3.2 Período de Responsabilidad del Adquiriente

La responsabilidad del ACVR del Adquiriente se calcula para el período del 1 de enero al 31 de diciembre. La responsabilidad del ACVR se determina después de la presentación final de las reclamaciones de reembolso por transacciones con tarjeta falsificada durante cada ciclo de 12 meses.

6.3.3.3 Relief from Liability

To qualify for relief from liability, an Acquirer must meet the following criteria:

1. The Acquirer must comply with the Acquirer loss control program Standards described in section 6.2.2.
2. The Acquirer must issue internal procedures designating responsibilities for monitoring the exception reports, explaining how they should be used, and defining actions to be taken when thresholds are exceeded. Customers will need to maintain internal records that clearly demonstrate supervisory review of such procedures and the periodic review of results by senior management.
3. The Acquirer must transmit the full, unedited ISO:8583 authorization message from terminal-read Transactions to the system.
4. The Acquirer that is subject to liability may be required by MasterCard to take additional action to attempt further to reduce its level of counterfeit losses.

MasterCard will provide relief from reversal of responsibility to Acquirers that exceed the threshold under the Acquirer Counterfeit Liability Program and that fully meet the aforementioned criteria.

NOTA: Acquirers must submit a written application for relief in order for MasterCard to provide relief from responsibility.

6.3.3.4 Solicitud de Exoneración

El Adquiriente debe presentar una solicitud de exoneración por escrito firmada por un funcionario adecuado, como el Gerente del Centro de Tarjetas de ese Cliente. Se deberá incluir la siguiente información en la solicitud:

- Certificación de que los controles requeridos se han puesto en práctica

- Descripción detallada de los controles
- Parámetros específicos utilizados
- Una copia del documento de los procedimientos descrito en la sección 6.3.3.3
- Copias de muestra de los informes de excepción automatizados

La solicitud de exoneración debe enviarse al vicepresidente de los Servicios de Seguridad y Riesgos a la dirección proporcionada en el Apéndice B.

La fecha de vigencia de las disposiciones de exoneración será de no menos de 90 días después de que el Adquiriente haya implementado los controles requeridos de forma completa. No se concederá la exoneración de responsabilidad al Adquiriente hasta que se cumpla con todos los requisitos al menos por 90 días. La continua elegibilidad para la exoneración estará sujeta a revisiones periódicas por parte del personal de Servicios de Seguridad y Riesgos, y podrá ser revocada en cualquier momento.

6.4 Programa de Control de Pérdidas del Emisor de Maestro (LCP)

Un Emisor debe implementar estrategias eficaces de control de fraude a fin de proteger la reputación e integridad de la marca Maestro.

El Programa de Control de Pérdidas del Emisor de Maestro (LCP) se centra en los tres grupos a continuación:

- Emisores del Grupo 1—Emisores con controles geográficos dinámicos
- Emisores del Grupo 2—Emisores sin controles geográficos dinámicos
- Emisores del Grupo 3—Emisores que experimentan fraude que supera los niveles establecidos

MasterCard puede exigir a un Cliente implementar medidas además de los requisitos mínimos establecidos en esta sección.

6.4.1 Group 1 Issuers—Issuers with Dynamic Geo-Controls

A Group 1 Issuer is an Issuer with a dynamic geo-control solution in place. A Group 1 Issuer typically:

1. Places each Cardholder into a defined segment of the Issuer's Portfolio based on the Cardholder's recent travel behavior, for example:
    a. Cardholders that travel outside of the Issuer's Region ("Interregional Cardholders")
    b. Cardholders that travel outside of the country of Card issuance but not outside of the Issuer's Region ("Intraregional Cardholders")
    c. Cardholders that do not travel outside of the country of Card issuance ("Domestic Cardholders")
    d. Affluent ("VIP") Cardholders, Cardholders that reside abroad, and frequent travelers
2. Implements daily and weekly spending limits for high-risk Transactions, per defined Portfolio segment.

3. Offers a variety of channels by which a Cardholder may switch from one segment to another.
4. Regularly optimizes segment definitions and spending profiles to achieve the best balance between Card utility and fraud reduction.

NOTA:

This strategy is particularly relevant to Maestro Chip Card Issuers operating in Regions where EMV migration is advanced or complete. In this situation, the majority of Intraregional Transactions and Interregional Transactions conducted in a face-to-face environment are Chip Transactions.

A Group 1 Issuer may contact its local Customer Fraud Management representative to discuss the implementation of additional controls.

6.4.2 Emisores del Grupo 2 —Emisores sin Controles Geográficos Dinámicos

Un Emisor del Grupo 2 es un Emisor que no tiene una solución de control geográfico dinámica. Un Emisor del Grupo 2 debe implementar los siguientes controles mínimos.

6.4.2.1 Authorization Controls

A Group 2 Issuer must implement a rules-based authorization strategy. The strategy must be regularly reviewed and updated as appropriate. Spending limits set by the Issuer within its authorization strategy should be set to have minimum impact on valid Transactions and maximum impact on fraud reduction.

A Group 2 Issuer must include the following parameters in its authorization system:

- A single Transaction exceeding a certain amount (established by the Issuer)
- Multiple Transactions exceeding a certain amount (established by the Issuer)

The Issuer should set specific limits with respect to:

- High-risk MCCs;
- Particular Merchant locations determined to be high-risk;
- Particular POS entry modes (for example, magnetic stripe-read, chip-read, or key-entered); and
- Particular country codes.

A Group 2 Issuer should also include rules and parameters based on authorization and clearing data relating to the following:

- Account-generated attacks
- CVC 1, CVC 2, and CVC 3 validation failures
- PIN, MasterCard® *SecureCode*™ token, or ARQC validation failures
- Mismatches between "Card Verification Results (CVR)" in the Issuer Application Data of Data Element (DE) 55 and "CVM Results"
- Expiration date failures
- Invalid Account number (mis-posted) Transactions

- Unattended POS Terminal Transactions
- ADC Event or Potential ADC Event Transactions
- Refund Transactions and Merchant authorization reversals
- Dormant Card list (monthly)

A Group 2 Issuer should also:

1. Monitor authorization data, including the use of real-time alerts;
2. In a dual message environment, monitor clearing data; and
3. Generate daily reports, at the latest on the day after the monitored Transaction(s) occur or are received through clearing.

6.4.3 Group 3 Issuers—Issuers Experiencing Fraud in Excess of Established Levels ("High Fraud")

A Group 3 Issuer is any Issuer (regardless of whether the Issuer satisfies the definition of a Group 1 Issuer or Group 2 Issuer) that meets either of the following criteria for fraud in excess of established levels ("high fraud"):

1. The Issuer's Maestro Transaction fraud basis points in any month exceed two times the Regional average or two times the worldwide average; and/or
2. The Issuer's total fraud in any month within fraud types required to be reported to SAFE exceeds a figure set by MasterCard.

A Group 3 Issuer may be:

1. Contacted by its local Customer Fraud Management representative to establish an action plan for achieving compliance with the Standards, including the implementation of recommended fraud reduction measures; and/or
2. Required to undertake a Global Risk Management Program review; and/or
3. Required to deploy a dynamic geo-control or other appropriate fraud management solution.

A Group 3 Issuer experiencing high fraud for three consecutive months may be prohibited from submitting more than seven fraud-related chargebacks involving the same Maestro Account (for purposes of this rule, "Account" means the PAN and expiration date). If an Issuer fails to take appropriate fraud reduction measures within a specified time period and continues to experience high fraud, the Issuer may be prohibited from charging back Maestro Transactions using message reason code 70 or 4870 (Chip Liability Shift). Any such Issuer will be listed in the *Global Security Bulletin* during the period of chargeback limitation. A listed Issuer may, at any time, request an audit by MasterCard of the adequacy of its fraud and security controls and its removal from the *Global Security Bulletin* listing.

6.4.4 Implementación de la Herramienta de Detección de Fraude

Cada Emisor de Maestro debe implementar una herramienta de detección de fraude eficaz para limitar cualquier fraude a un volumen que esté dentro de los niveles establecidos, tal como se describe en la sección 6.4.3.

La herramienta de detección de fraude debe lograr los requisitos mínimos de desempeño. Los indicadores de desempeño deben incluir, entre otros, las tasas de detección de fraude de la Cuenta, el número promedio de Transacciones por caso de fraude, la duración promedio del caso de fraude, y la pérdida promedio por caso de fraude.

6.4.5 Cardholder Communication Strategy

Each Maestro Issuer must implement a Cardholder communication strategy. A communication strategy consists of defining (i) the criteria for contacting a Cardholder, (ii) the communication channel for contacting the Cardholder, and (iii) the actions to be taken in case of failure to contact the Cardholder. Such communication channels may include SMS alerts, email messages, phone calls, and letters.

Capítulo 7 Normas de Investigación y Control de Comercios, Comercios Secundarios y Propietarios de ATM

Este capítulo puede ser de interés especial para el personal del Cliente responsable de investigar y controlar a los Comercios, Comercios Secundarios y Propietarios de ATM.

7.1 Investigación de Comercios, Comercios Secundarios y Propietarios de ATM Nuevos

Un Cliente es responsable de asegurar que los procedimientos descritos en esta sección para la investigación de un posible Comercio, Comercio Secundario o Propietario de ATM se realicen antes de que el Cliente celebre un Convenio de Comercio o un Convenio de Propietario de ATM o que un Facilitador de Pagos del Cliente celebre un Convenio de Comercio Secundario.

La realización de estos procedimientos de investigación no exime a un Cliente de la responsabilidad de seguir las buenas prácticas bancarias comerciales. La revisión de un reporte anual o de un estado de cuenta auditado, por ejemplo, puede sugerir la necesidad de una investigación más amplia.

7.1.1 Merchant Screening Procedures

Each Acquirer, before entering into a Merchant Agreement with a Merchant, must verify that the prospective Merchant is a bona fide business. Such verification must include at least all of the following:

- For each prospective Merchant with more than USD 100,000 in projected or actual annual combined MasterCard and Maestro Point-of-Sale (POS) Transaction volume, conduct a credit check (such as by obtaining a credit report from a credit bureau). If the credit check raises questions or does not provide sufficient information, the Acquirer also should conduct a credit check of:
  - The owner, if the prospective Merchant is a sole proprietor; or
  - The partners, if the prospective Merchant is a partnership; or
  - The principal shareholders, if the prospective Merchant is a corporation.

  A credit check must also be performed if required by applicable law or regulation.
- Perform background investigations and reference checks of the prospective Merchant.
- Check for the validity of the business address and other information provided by the prospective Merchant.
- Submit an inquiry to the MasterCard Alert to Control High-risk (Merchants) (MATCH™) system if the prospective Merchant proposes to accept MasterCard Cards. The MATCH inquiry for a prospective Merchant proposing to conduct electronic commerce (e-commerce) Transactions must include the Universal Resource Locator (URL) address of its website.
- Investigate the prospective Merchant's previous and other relationships with Customers or Payment Facilitators, if any.

NOTA: A Customer must participate in the MATCH system unless excused by MasterCard or prohibited by law.

An Acquirer is not required to conduct a credit check of a public or private company that has annual sales revenue in excess of USD 50 million (or the foreign currency equivalent), provided

the Acquirer reviews, and finds satisfactory for purposes of the acquiring being considered, the most recent annual report of the Merchant, including audited financial statements. A private company that does not have a recent audited financial statement is subject to a credit check and inspection even if its annual sales revenue exceeds USD 50 million.

As a best practice, the Acquirer also should:

- Inspect the prospective Merchant's premises (both physical locations and Internet URLs, as applicable) and records to ensure that the prospective Merchant has the proper facilities, equipment, inventory, agreements, and personnel required and if necessary, license or permit and other capabilities to conduct the business.
- Ensure that the prospective Merchant is able to support the provision of products or services to be marketed, and has procedures and resources to timely and appropriately respond to Cardholder inquiries and to support refund requests.

7.1.2 Procedimientos de Investigación de los Comercios Secundarios

Cada Facilitador de Pagos, antes de firmar un Convenio de Comercio Secundario, debe verificar que el posible Comercio Secundario sea un negocio de buena fe. Dicha verificación deberá incluir todo lo siguiente:

- Para cada posible Comercio Secundario con más de USD 100.000 en volumen de Transacción de POS de MasterCard y Maestro combinado, anual real o proyectado, deberá realizar una verificación de crédito (tal como al obtener un informe crediticio de una oficina de crédito). Si la verificación de crédito arroja dudas o no proporciona la suficiente información, el Facilitador de Pagos deberá efectuar también una verificación de crédito de:
  - El propietario, si el posible Comercio Secundario es de un único propietario; o
  - Los socios, si el posible Comercio Secundario es una sociedad comercial; o
  - Los accionistas principales, si el posible Comercio Secundario es una corporación.

  También se debe realizar una verificación de crédito si lo exige el Adquiriente o la ley o reglamento aplicable.
- Realizar la investigación de antecedentes y verificación de referencias del posible Comercio Secundario.
- Revisar la validez de la dirección del negocio y otra información suministrada.
- Solicitar que el Adquiriente, para quien el Facilitador de Pagos es un agente, envíe una consulta al sistema MATCH™ si el posible Comercio Secundario propone aceptar las Tarjetas MasterCard (el propio Adquiriente debe realizar directamente la consulta al sistema MATCH). La consulta al MATCH sobre un posible Comercio Secundario que propone efectuar Transacciones de comercio electrónico debe incluir la dirección del URL del sitio web del posible Comercio Secundario.

NOTA:

Un Cliente debe participar en el sistema MATCH a menos que MasterCard lo exonere o que se prohíba por ley.

Como mejor práctica, el Facilitador de Pagos también deberá:

- Inspeccionar el establecimiento del posible Comercio Secundario (tanto las ubicaciones físicas como los URL de Internet, según corresponda) y los registros para asegurarse de que tiene las instalaciones, el equipamiento, inventario, personal y los convenios adecuados y requeridos y, si fuera necesario, la licencia o el permiso y otras capacidades para realizar negocios.
- Asegurarse de que el posible Comercio Secundario pueda apoyar el suministro de productos o servicios para el mercado y que tenga los procedimientos y recursos para responder de manera oportuna y adecuada a las consultas del Tarjetahabiente y para apoyar las solicitudes de reembolso.
- Investigar las relaciones anteriores y demás del posible Comercio Secundario con Clientes o Facilitadores de Pagos, si existieran.

El Adquiriente debe agregar a cada Comercio Secundario cancelado por cualquiera de los motivos descritos en la sección 11.5.1 al sistema MATCH.

7.1.3 ATM Owner Screening Procedures

Each Acquirer, before signing an ATM Owner Agreement with an ATM owner, must verify that the prospective ATM owner is a bona fide business. Such verification must include at least all of the following:

- Conduct a credit check (such as by obtaining a credit report from a credit bureau). If the credit check raises questions or does not provide sufficient information, the Acquirer also should conduct a credit check of:
  - The owner, if the prospective ATM owner is a sole proprietor; or
  - The partners, if the prospective ATM owner is a partnership; or
  - The principal shareholders, if the prospective ATM owner is a corporation.
- Perform background investigations and reference checks of the prospective ATM owner.
- Confirm that all ATMs claimed by a prospective ATM owner exist and are operational.
- Verify the location and condition of all ATMs deployed by a prospective ATM owner.

An Acquirer is not required to conduct a credit check of a prospective ATM owner public or private company that has annual sales revenue in excess of USD 50 million (or the foreign currency equivalent), provided the Acquirer reviews, and finds satisfactory for purposes of the acquiring being considered, the most recent annual report of the prospective ATM owner, including audited financial statements. A private company that does not have a recent audited financial statement is subject to a credit check and inspection even if its annual sales revenue exceeds USD 50 million.

As a best practice, the Acquirer also should perform an inspection of the prospective ATM owner's premises and records to ensure that it has the proper facilities, equipment, inventory, agreements, and personnel required and if necessary, license or permit and other capabilities to conduct the business.

7.1.4 Evidencia de Acatamiento a los Procedimientos de Investigación

Como evidencia de que el Adquiriente acata los requisitos de investigación establecidos en este capítulo, MasterCard requiere, como mínimo, la siguiente información:

- Un informe de una agencia de crédito o, si este informe no está disponible o es incompleto, los resultados por escrito de otras investigaciones financieras y verificaciones de antecedentes del negocio, sus principales propietarios y funcionarios;
- Con respecto a la investigación de un Comercio o Comercio Secundario para el procesamiento de las Transacciones en el POS de MasterCard, prueba de la consulta del Adquiriente al sistema MATCH, incluyendo una copia del registro de consultas;
- Con respecto a la investigación de un Comercio, una declaración del Comercio sobre los Convenios de Comercio anteriores, incluyendo el o los nombres de la o las entidades donde el Comercio tenga o haya tenido convenios y el o los motivos de cancelación de esos convenios, si corresponde.

7.1.5 Retention of Investigative Records

The Acquirer must retain all records concerning the investigation of a Merchant, Submerchant, or ATM owner for a minimum of two years after the date that the Merchant Agreement, Submerchant Agreement, or ATM Owner Agreement, as applicable, is terminated or expires. MasterCard recommends that Acquirers retain the following records as a best practice:

- Signed Merchant Agreement
- Previous Merchant statements
- Corporate or personal banking statements
- Credit reports
- Site inspection report, to include photographs of premises, inventory verification, and the name and signature of the inspector of record
- Merchant certificate of incorporation, licenses, or permits
- Verification of references, including personal, business, or financial
- Verification of the authenticity of the supplier relationship for the goods or services (invoice records) that the Merchant is offering the Cardholder for sale
- Date-stamped MATCH inquiry records
- Date-stamped MATCH addition record
- All Customer correspondence with the Merchant or ATM owner
- All correspondence relating to Issuer, Cardholder, or law enforcement inquiries concerning the Merchant, Submerchant, ATM owner, or any associated Service Provider
- Signed Service Provider contract, including the name of agents involved in the due diligence process
- Acquirer due diligence records concerning the Service Provider and its agents

Refer to Chapter 7 of the *MasterCard Rules* manual for more information about Service Providers.

NOTA: MasterCard recommends that the Acquirer retain these records to verify compliance with the screening procedures, in the event that MasterCard conducts an audit as described in section 7.1.6.

7.1.6 Recargos por No Acatamiento de los Procedimientos de Investigación

MasterCard puede auditar a un Adquiriente sobre el acatamiento de los procedimientos de investigación descritos en este capítulo, y cada Cliente debe acatar y ayudar en dicha auditoría. MasterCard revisará los registros correspondientes retenidos por el Adquiriente para determinar si un Adquiriente ha acatado estos procedimientos de investigación.

Si MasterCard determina que un Adquiriente no ha acatado estos procedimientos de investigación y si el Adquiriente no corrige todas las deficiencias que dieron lugar a la violación, a satisfacción de MasterCard, dentro de los 30 días de haberse conocido o advertido de estas deficiencias, MasterCard podrá imponer un recargo de hasta USD 100.000 al Adquiriente por cada período de 30 días luego del período mencionado anteriormente, con un recargo máximo total de USD 500.000 durante cualquier período de 12 meses consecutivos. Cualquier recargo(s) como éste será adicional a cualquier otra responsabilidad financiera en la que el Adquiriente pueda incurrir, según se estipula en las Normas. Quienes violen estas normas también estarán sujetos a contracargos de Transacciones fraudulentas.

Si no se consulta al sistema MATCH antes de firmar el Convenio de Comercio para el procesamiento de Transacciones de POS de MasterCard o antes de que un Facilitador de Pagos firme un Convenio de Comercio secundario para el procesamiento de Transacciones de POS de MasterCard, resultará en un recargo de hasta USD 5.000 por cada caso de no acatamiento.

7.2 Control Permanente

El Adquiriente debe controlar y confirmar regularmente que la actividad de Transacción de cada uno de sus Comercios (ventas, créditos y contracargos) se efectúe de forma legal y ética y en acatamiento total de las Normas, y asegurarse de que un Facilitador de Pagos realice dicho control con relación a cada uno de sus Comercios Secundarios, en un esfuerzo por impedir el fraude. El control debe enfocarse en los cambios de la actividad con el transcurso del tiempo, las inconsistencias en las actividades comerciales del Comercio o Comercio Secundario, o en las actividades poco comunes relacionadas con el número de Transacciones y los montos de las Transacciones fuera de lo común relacionadas con las ventas de temporada. Específicamente para el procesamiento de Transacciones de POS de MasterCard, el control continuo incluye, entre otros, controles de pérdidas por fraude del Adquiriente relacionados con las actividades de depósito (que incluyen créditos) y de autorización descritas en la sección 6.2.2.

Con respecto a un Comercio de comercio electrónico, el Adquiriente, según sea razonablemente adecuado y teniendo en cuenta todas las circunstancias, debe revisar y controlar regularmente el sitio o sitios web del Comercio y las actividades comerciales para confirmar y reconfirmar con frecuencia que cualquier actividad relacionada con o que utiliza una Marca se realice de manera legal y ética, y en completo acatamiento de las Normas. El

Adquiriente debe garantizar que un Facilitador de Pagos realice dicho control con respecto a cada uno de los sitios web de su Comercio Secundario.

Como una mejor práctica, MasterCard recomienda a los Adquirientes usar una solución de control del Comercio para revisar la actividad de comercio electrónico de sus Comercios y Comercios Secundarios con el fin de evitar el procesamiento de Transacciones ilegales o que perjudiquen la marca.

7.3 Educación a Comercios

Una vez que se establece una relación de adquisición, un Adquiriente debe establecer un programa de prevención de fraude, incluyendo un proceso de educación que consista de visitas periódicas a los Comercios, distribución de bibliografía educativa relacionada y participación en seminarios de Comercios. Las instrucciones a los comercios deben incluir los procedimientos de aceptación de Tarjetas, el uso del Archivo del Electronic Warning Bulletin o la *Notificación de Advertencia*, los procedimientos de autorización, incluyendo los procedimientos del Código 10, los documentos de información de la Transacción (TID) debidamente completados (incluyendo el truncamiento del número de cuenta primario [PAN]), la presentación a tiempo de la Transacción al Adquiriente y el manejo adecuado conforme a las solicitudes de retención de Tarjetas. Los clientes deberán revisar exhaustivamente con los Comercios las Normas contra la presentación de Transacciones fraudulentas. Además, los Clientes deben revisar los procedimientos de seguridad de los datos para asegurarse de que se almacenen solamente los datos apropiados de la Tarjeta, que nunca se almacenen los datos de la banda magnética y que cualquier almacenamiento de datos se haga conforme a las Normas de encriptado, procesamiento de las Transacciones y otras prácticas establecidas.

Un Adquiriente debe asegurarse también de que un Facilitador de Pagos efectúe actividades de educación adecuadas con cada uno de sus Comercios Secundarios.

7.4 Requisitos Adicionales para Determinadas Categorías de Comercios y Comercios Secundarios

El Adquiriente de un Comercio o Comercio Secundario de contenido y servicios para adultos que no es cara a cara, Comercio o Comercio Secundario de juegos de azar que no es cara a cara, Comercio o Comercio Secundario de productos farmacéuticos o de tabaco que no es cara a cara, Comercio o Comercio Secundario de lotería gubernamental, Comercio o Comercio Secundario de juegos de habilidades (región de EE. UU. solamente), Comercio o Comercio Secundario de cyberlocker de alto riesgo y/o Comercio o Comercio Secundario informado bajo el Programa de Exceso de Contracargos (ECP) debe acatar los requisitos de inscripción y control del Programa de Inscripción de MasterCard (MRP) para cada Comercio o Comercio Secundario, según se describe en el Capítulo 9.

Capítulo 8 Programas de Control de Fraude de MasterCard

Este capítulo puede ser de interés especial para el personal del Cliente responsable de controlar la actividad del Comercio y/o del Emisor en cuanto al acatamiento de las Normas de control de pérdidas por fraude.

8.1 Cómo Notificar a MasterCard

Esta sección describe los requisitos de la presentación de informes de Control de Fraude del Comercio.

8.1.1 Responsabilidades del Adquiriente

Si un Adquiriente tiene motivos para creer que un Comercio con el cual ha celebrado un Convenio de Comercio de MasterCard participa en actividades de confabulación o de otro modo fraudulentas o inadecuadas, debe notificar inmediatamente al personal de Control de Fraude del Comercio usando la información proporcionada en el Apéndice B.

8.1.2 Responsabilidades del Emisor

Si un Emisor se entera de que un Comercio viola la Regla 5.12 del manual *Reglamento de MasterCard* ("la Regla de las Transacciones Válidas"), a través de quejas de un Tarjetahabiente o de otro modo, deberá notificar inmediatamente al personal de Control de Fraude del Comercio usando la información proporcionada en el Apéndice B.

8.2 Global Merchant Audit Program

The Global Merchant Audit Program (GMAP) uses a rolling six months of data to identify MasterCard Merchant locations that, in any calendar month, meet the criteria set forth in Table 8.1.

Table 8.1—Fraud Criteria for Global Merchant Audit Program Tier Classification

A MasterCard Merchant location is classified in the following GMAP tier...	If in any calendar month, the MasterCard Merchant location meets the following fraud criteria...
Tier 1—Informational Fraud Alert	• Three fraudulent Transactions • At least USD 3,000 in fraudulent Transactions • A fraud-to-sales dollar volume ratio minimum of 3% and not exceeding 4.99%
Tier 2—Suggested Training Fraud Alert	• Four fraudulent Transactions • At least USD 4,000 in fraudulent Transactions • A fraud-to-sales dollar volume ratio minimum of 5% and not exceeding 7.99%

A MasterCard Merchant location is classified in the following GMAP tier...	If in any calendar month, the MasterCard Merchant location meets the following fraud criteria...
Tier 3—High Fraud Alert	• Five fraudulent Transactions • At least USD 5,000 in fraudulent Transactions • A fraud-to-sales dollar volume ratio minimum of 8%

If a MasterCard Merchant location is identified in multiple tiers during any rolling six-month period, GMAP will use the highest tier for the Merchant identification.

NOTA: If a MasterCard Merchant has more than one location (or outlet), the program criteria apply to each location independently.

8.2.1 Responsabilidades del Adquiriente

MasterCard notificará a un Adquiriente sobre la identificación de un Comercio de Nivel 1, Nivel 2 o Nivel 3 por medio de la herramienta de Rastreo en Línea del Estado del Comercio (MOST). Las identificaciones del Comercio por parte del GMAP se proporcionan solamente con fines informativos y no es necesaria la respuesta del Adquiriente. Si MasterCard notifica a un Adquiriente por medio del MOST que se ha iniciado la auditoría especial de un Comercio de Nivel 3, el Adquiriente debe responder según se describe en la sección 8.2.2.

Cuando se identifica a un Comercio de Nivel 1, Nivel 2 o Nivel 3, el Adquiriente deberá evaluar las medidas de control de fraude y los procedimientos de capacitación de Comercios existentes para ese Comercio. MasterCard recomienda encarecidamente que el Adquiriente actúe en forma oportuna a fin de corregir cualquier deficiencia identificada. Las mejoras sugeridas se describen en la *GMAP Best Practices Guide for Acquirers and Merchants to Control Fraud*.

MasterCard puede efectuar, a su entera discreción, una auditoría a fin de determinar si el establecimiento de un Comercio viola la Regla de Transacciones Válidas, según se describe en la sección 5.12 del *Reglamento de MasterCard*, y podrá asignar la responsabilidad del contracargo.

8.2.2 Auditoría Especial del Comercio de Nivel 3

Si el GMAP identifica al establecimiento de un Comercio en la Escala 3, MasterCard determinará si iniciar una auditoría del establecimiento del Comercio ("una auditoría especial al Comercio de Nivel 3"). Si MasterCard decide efectuar una auditoría especial del Comercio de Nivel 3, el procedimiento se efectuará de la siguiente manera:

1. **MasterCard notifica al Adquiriente.** El Adquiriente recibirá una notificación de MasterCard, a través del MOST, sobre el inicio de una auditoría especial al Comercio de Nivel 3.

2. **El Adquiriente deberá enviar una respuesta dentro de un período de 30 días.** A más tardar 30 días después de la fecha de notificación de la auditoría especial al Comercio de Nivel 3 ("período de respuesta de 30 días"), el Adquirente debe responder a la notificación de la auditoría a través del MOST, ya sea mediante:

   a. Notificación a MasterCard sobre que el Adquiriente ha cancelado al Comercio (si el Adquiriente determina que se debe informar al Comercio al sistema MATCH, el Adquiriente podrá hacerlo a través del MOST), o;
   b. Cuestionario en línea completado, si el Adquiriente no canceló al Comercio. Este cuestionario se usa para informar a MasterCard de: 1) cualquier circunstancia excepcional o atenuante con relación al fraude del Comercio identificado y 2) las medidas de control de fraude implementadas en el establecimiento del Comercio.

   Tras revisar el cuestionario completado en línea, MasterCard, a su entera discreción, podrá:

   – Conceder una exclusión al establecimiento del Comercio para la identificación del Comercio, o;
   – Brindar al Adquiriente la oportunidad de implementar medidas de control de fraude adicionales ("el plan de acción de control de fraude"), según las indicaciones de MasterCard, en el establecimiento del Comercio, o;
   – Asignar la responsabilidad de los contracargos al Adquiriente para el establecimiento del Comercio.
3. **Plan de acción de control de fraude requerido dentro del período de acción de 90 días.** Si MasterCard requiere que el Adquiriente implemente un plan de acción de control de fraude, MasterCard proporcionará el plan al Adquiriente a través del MOST. El Adquiriente tiene 90 días desde el primer día del mes siguiente al mes en el cual se identificó al Comercio en el GMAP ("el período de acción de 90 días") para tomar todas las medidas requeridas, incluyendo, entre otras, la confirmación de que se ha implementado dicho plan de acción de control de fraude. MasterCard podrá extender, a su entera discreción, el período de acción de 90 días. Para los Adquirientes que implementan un plan de acción de control de fraude, el Comercio identificado será nuevamente elegible para ser identificado en el GMAP, a partir del sexto mes posterior al mes en el cual el se identificó por primera vez al Comercio en el GMAP. Las Transacciones Fraudulentas informadas al SAFE serán revisadas bajo el Programa a partir del cuarto y quinto mes posterior al mes en el cual se identificó al Comercio en el GMAP, y continuará de forma incremental a partir de ese momento hasta que el se complete un período de revisión continuo de seis meses al Comercio, siempre y cuando el Comercio no sobrepase los márgenes de Nivel 1, 2 ó 3 del GMAP.

El Adquiriente de un Comercio sujeto a una auditoría especial de Comercio de Nivel 3 deberá proporcionar la documentación necesaria a fin de probar que se han implementado controles razonables para combatir el fraude, incluyendo la implementación de un plan de acción de control de fraude dirigido por MasterCard.

Consulte la Figura 8.1 para ver un cronograma de muestra de una auditoría especial a un Comercio de Nivel 3.

Figura 8.1—Cronograma de Muestra de una Auditoría Especial a un Comercio de Nivel 3

<table>
<tr><td colspan="2">February</td><td>Month 1
March</td><td>Month 2
April</td><td>Month 3
May</td><td>Month 4
June</td><td>Month 5
July</td><td>Month 6
August</td></tr>
<tr><td colspan="2"></td><td colspan="2">30-DAY RESPONSE PERIOD
15 February to 15 March</td><td></td><td colspan="3">After the implementation of the fraud control action plan, GMAP reviews SAFE reported fraudulent transactions for Months 4 and 5, and incrementally thereafter until a rolling six months is resumed.
(For example, in Month 6, GMAP reviews fraud in Months 4 and 5.)</td></tr>
<tr><td colspan="2"></td><td colspan="3">90-DAY ACTION PERIOD
1 March to 30 May</td><td colspan="3"></td></tr>
<tr><td colspan="2">2 February
GMAP identifies a merchant in Tier 3. MasterCard conducts a review of fraud criteria.

15 February
By this date, MasterCard is expected to have notified the acquirer that a Tier 3 special merchant audit has been initiated.</td><td>15 March
The end of the 30-day response period. The acquirer must respond in MOST by either indicating that the merchant has been terminated or by completing the online questionnaire through MOST.

30 March
By this date, MasterCard is expected to have determined whether further action is required, and if so, provide a fraud control action plan.</td><td>31 March to 29 May
The acquirer implements the fraud control action plan.</td><td>30 May
By this date, the acquirer must have implemented the fraud control action plan at the merchant location. MasterCard requires the acquirer to confirm successful implementation.</td><td>Fraud reported to SAFE becomes eligible for GMAP identification.</td><td>Fraud reported to SAFE becomes eligible for GMAP identification.</td><td>Merchant is eligible for GMAP identification.</td></tr>
<tr><td colspan="5"></td><td colspan="3">CHARGEBACK LIABILITY PERIOD
MasterCard may list the merchant in a Global Security Bulletin, thereby alerting issuers that the acquirer will be responsible for chargebacks.
The six-month period will be from 1 June through 30 November.</td></tr>
</table>

8.2.3 Responsabilidad del Contracargo

MasterCard efectuará una revisión a cada Adquiriente de un establecimiento de Comercio sujeto a una auditoría especial de Comercio de Nivel 3, caso por caso, y determinará, a la entera discreción de MasterCard, si aplica un período de responsabilidad del contracargo. El período de responsabilidad del contracargo es por seis meses y comienza el primer día del cuatro mes posterior a la identificación de Nivel 3 del GMAP.

MasterCard, a su entera discreción, podrá extender el período de responsabilidad del contracargo a 12 meses.

MasterCard se reserva el derecho de listar la Identificación del Adquiriente, el nombre del Adquiriente, el nombre del Comercio, el establecimiento del Comercio y el período de responsabilidad del contracargo de cualquier Comercio de Nivel 3 en un *Boletín de Seguridad Global*.

Cuando MasterCard lista la información del Adquiriente y del Comercio en un *Boletín de Seguridad Global*, aplicarán los derechos de contracargo del Emisor. Después cada Emisor tiene derecho a usar el código de motivo de mensaje 4849—Actividad Sospechosa del

Comercio para contracargar al Adquiriente las Transacciones fraudulentas del Comercio que se comunican al SAFE con los siguientes tipos de fraude:

- 00—Fraude con Tarjeta Extraviada,
- 01—Fraude con Tarjeta Robada,
- 04—Fraude con Tarjeta Falsificada,
- 06—Sin Tarjeta Presente Fraude, o
- 07—Fraude por Impresiones Múltiples.

Cada Transacción contracargada debe haberse efectuado durante el período del contracargo publicado, y debe comunicarse al SAFE dentro del plazo límite correspondiente (consulte el Capítulo 12 de este manual). Los emisores no deben usar el código de motivo de mensaje 4849 para contracargar Transacciones de un Adquiriente y un Comercio identificados en el GMAP si el tipo de fraude es:

- 02—Emitida Nunca Recibida,
- 03—Solicitud Fraudulenta,
- 05—Fraude por Usurpación de Cuenta, o
- 51—Comercio en Confabulación de Fraude de Bust-out.

Después de que MasterCard lista la Identificación del Adquiriente, el nombre del Adquiriente, el nombre del Comercio, el establecimiento del Comercio y el período de responsabilidad del contracargo en un *Boletín de Seguridad Global*, el Emisor no podrá usar el código de motivo de mensaje 4849—Actividad Sospechosa del Comercio, en ninguna de las siguientes situaciones:

- La Transacción no se comunicó correctamente al SAFE dentro del plazo límite correspondiente especificado en este manual.
- La Transacción se comunicó al SAFE como un tipo de fraude de Tarjeta Emitida Nunca Recibida (02), Solicitud Fraudulenta (03), Fraude por Usurpación de Cuenta (05) o Comercio en Confabulación de Fraude de Bust-out (51).
- Si el cambio de responsabilidad global de *SecureCode* para las Transacciones de comercio electrónico está vigente, y ocurren todas las condiciones siguientes:
  - El Comercio tiene capacidad para el Campo Universal de Autenticación del Tarjetahabiente (UCAF™), y
  - El Emisor proporcionó los datos del UCAF para esa Transacción, y
  - Se cumplieron todos los demás requisitos del mensaje de Solicitud de Autorización/0100 y los requisitos de compensación de comercio electrónico, y
  - El mensaje de Respuesta de Solicitud de Autorización/0110 reflejó la aprobación de la Transacción del Emisor.
- Si está vigente un cambio de responsabilidad del chip nacional o dentro de la región, o el Programa de Cambio de Responsabilidad del Chip entre regiones (Nivel 1), la Transacción fue procesada en una Terminal que acataba las normas del chip, se comunicó la Transacción al SAFE como fraude por falsificación, y se identificó la Transacción

[3] Consulte las restricciones del Emisor a los contracargos por el código de motivo de mensaje 4849 para el cambio de responsabilidad global de MasterCard® *SecureCode*™, según se describe más adelante en esta sección.

correctamente como 1) una Transacción con chip fuera de línea en el registro de compensación, o 2) una Transacción en línea en el mensaje de Solicitud de Autorización/0100, y el mensaje de Respuesta de Solicitud de Autorización/0110 reflejó la aprobación de la Transacción por parte del Emisor.

8.2.4 Exclusión del Programa Global de Auditoría del Comercio

Las siguientes secciones abordan exclusiones del GMAP.

8.2.4.1 Exclusiones Sistemáticas

Las siguientes Transacciones se excluyen sistemáticamente con el fin de determinar la identificación de un Comercio en el GMAP:

- **Fraude de Débito**—Esto incluye todas las transacciones de fraude relacionadas con Cirrus (CIR) y Maestro (MSI).
- **Todos los tipos de fraude de Tarjeta Emitida Nunca Recibida, Solicitud Fraudulenta, Usurpación de Cuenta (ATO), y Comercio en Confabulación de Fraude de Bust-out**—Esto incluye a todas las Transacciones comunicadas al SAFE como tipo de fraude:
  - 02—Tarjeta Emitida Nunca Recibida
  - 03—Solicitud Fraudulenta
  - 05—Fraude por Usurpación de Cuenta
  - 51—Comercio en Confabulación de Fraude de Bust-out

8.2.4.2 Exclusión Después de la Identificación del GMAP

Luego de que MasterCard notifica a un Adquiriente sobre el inicio de la auditoría especial a un Comercio de Nivel 3, el Adquiriente puede solicitar que MasterCard excluya al Comercio por una buena causa.

Al solicitar una exclusión, el Adquiriente debe enviar el cuestionario en línea de la auditoría especial al Comercio completado dentro de los 30 días posteriores a la notificación de la auditoría especial al Comercio de Nivel 3 y proporcionar cualquier otra información de apoyo que MasterCard solicite.

El personal de MasterCard decidirá si excluye a un Comercio del GMAP.

Cuando evalúa las solicitudes de exclusión, MasterCard podrá tener en cuenta los siguientes puntos:

- **Una proporción en dólares del volumen de fraude sobre las ventas por debajo del 8 por ciento**—Si el volumen en dólares de MasterCard del Comercio no está disponible para el cálculo en forma sistemática, el Adquiriente tendrá la oportunidad de proporcionar estos datos a MasterCard para su revisión. A fin de recalcular la proporción en dólares del volumen de fraude sobre las ventas del Comercio, el Adquiriente debe presentar la documentación de apoyo para mostrar solamente las ventas de MasterCard del establecimiento identificado durante los meses aplicables en los que se cumplan los criterios de la identificación.

Si la documentación de apoyo demuestra que el establecimiento del Comercio no sobrepasó los márgenes de fraude de Nivel 3, el Adquiriente recibirá una exclusión para el Comercio.

Si la documentación de apoyo demuestra que la proporción del fraude frente a las ventas del Comercio excede el 8 por ciento, MasterCard tomará las medidas según se describen en la sección 8.2.2.

- **Programa de control de fraude vigente actualmente en el establecimiento del Comercio**—MasterCard revisará la información con relación al Programa de control de fraude actualmente vigente en el establecimiento del Comercio a fin de establecer si medidas adicionales de control de fraude hubieran podido evitar o disminuir el fraude.
- **Cadena de Comercio**—Una cadena de Comercio se encuentra definida en el manual *Formatos de Compensación de IPM* bajo el Elemento de Datos (DE) 43 (Nombre/Ubicación del Aceptador de Tarjetas) como uno de múltiples establecimientos de un Comercio que tienen el mismo dueño y que venden la misma línea de bienes o servicios. Las Normas de MasterCard señalan además que el campo secundario 1 (Nombre del Aceptador de Tarjetas) de este elemento de datos debe contener un identificador único al final de este campo si el Comercio tiene más de un establecimiento en la misma ciudad. Es responsabilidad del Adquiriente asegurarse de que todos los Comercios de esta naturaleza sean identificados adecuadamente. Los comercios con múltiples establecimientos que acatan esta Norma se identifican de manera exclusiva en los programas de auditoría.

  Los adquirientes con un Comercio sujeto a una auditoría especial al Comercio de Nivel 3 con base en un cálculo que incluye más de un establecimiento pueden solicitar una exclusión. Para solicitar dicha exclusión, el Adquiriente debe proporcionar a MasterCard los datos de ventas y de fraudes de cada establecimiento de la cadena. Si se utiliza el mismo número de Identificación del Comercio para identificar a todos los establecimientos del Comercio, el Adquiriente debe proporcionar además una copia del comprobante de venta de cada Transacción identificada como fraudulenta.

Exclusiones con base en otras circunstancias excepcionales o atenuantes—Un Adquiriente puede solicitar una exclusión del establecimiento de un Comercio de una auditoría especial al Comercio de Nivel 3, con base en circunstancias excepcionales o atenuantes proporcionando la información adecuada.

A continuación se muestran ejemplos de la información que MasterCard tendrá en cuenta con relación a una solicitud de exclusión por circunstancias excepcionales o atenuantes:

1. Error de datos del SAFE:
   - Monto informado de la Transacción Erróneo
   - Monto informado de la Transacción excesivo como resultado de la conversión de la moneda
   - La transacción se informó bajo la Identificación del Adquiriente o el nombre del Comercio incorrectos
   - Se comunicaron Transacciones Duplicadas
   - Transacción No Fraudulenta comunicada al SAFE por error (tal como una disputa)
2. El Comercio retuvo la Tarjeta(s) fraudulenta de una transacción en esta ubicación.

3. El Comercio ayudó en la captura y condena de un delincuente(es) que efectuó transacciones con Tarjetas fraudulentas en su ubicación.
4. El Comercio identificó Transacciones fraudulentas oportunamente, antes de haber despachado la mercancía y antes de haber emitido los créditos a la cuenta del Tarjetahabiente, siempre y cuando el crédito no haya sido emitido en respuesta a una solicitud de recuperación o de contracargo.

8.2.5 Notification of Merchant Identification

When a Merchant location is identified in GMAP, MasterCard will report the Merchant identification in MOST, detailing the identification.

In addition, the Acquirer will receive the Global Merchant Audit Program Report.

Acquirers must use MOST to respond to a Tier 3 special Merchant audit notification.

NOTA: Acquirers are responsible for ensuring that they are capable of receiving notification of Merchants identified in GMAP. If an Acquirer does not receive an automated notification, it is the Acquirer's responsibility to obtain this information through MasterCard Connect™.

8.2.5.1 Distribución de Informes

Consulte el *MOST Users' Manual* para obtener información sobre la distribución de los informes del GMAP.

8.2.6 Sistema de Rastreo En Línea del Estado del Comercio (MOST)

El sistema MOST reside en la plataforma de MasterCard Connect, y se utiliza para administrar el proceso de los Comercios identificados en el GMAP. El sistema MOST permite a un Adquiriente:

- Ver cada Comercio identificado en el GMAP
- Determinar los motivos por los cuales un Comercio fue identificado en el GMAP
- Recuperar los detalles completos de las Transacciones de cada Comercio identificado por medio del Fraud Reporter
- Ver el estado de cada Comercio sujeto a una auditoría especial de Comercio de Nivel 3
- Completar un cuestionario en línea según el requisito de MasterCard para una auditoría especial de Comercio de Nivel 3
- Determinar el período de responsabilidad del contracargo de cada Comercio sujeto a una auditoría especial de Comercio de Nivel 3

8.2.6.1 Mandato del Sistema MOST

Los adquirientes deben utilizar el sistema del MOST disponible en MasterCard Connect cuando sea requerido por MasterCard para responder a una auditoría de Comercio Especial de Nivel 3 en el MOST. MasterCard cobrará un cargo de procesamiento de USD 100 por cada identificación del Comercio para un Adquiriente que no utilice únicamente el MOST para responder a una auditoría de Comercio especial de Nivel 3.

MasterCard impondrá un cargo de procesamiento de USD 100 solamente una vez por cada respuesta de auditoría de Comercio especial de Nivel 3 requerida. El cargo será cobrado mediante un débito a la cuenta del Adquiriente del Sistema de Facturación Consolidada de MasterCard (MCBS).

Además, MasterCard puede imponer un cargo de procesamiento de USD 100 a un Adquiriente si la respuesta de auditoría del Comercio especial de Nivel 3 se completa en el MOST y se presenta utilizando cualquier otro método adicional. Sin embargo, MasterCard no impondrá un cargo de procesamiento al Adquiriente si responde a una auditoría de Comercio especial de Nivel 3 mediante el MOST y luego elije presentar la documentación de apoyo a través de otro método de comunicación, o entablar un diálogo con el personal de MasterCard.

Los sistemas MOST y MATCH se han incorporado en un conjunto de productos obligatorios por los cuales se les aplica a los Adquirientes globalmente un cargo anual combinado de USD 5.000.

8.2.6.2 Inscripción en el Sistema MOST

Para usar el MOST, un usuario debe tener licencia para cada número de Cliente/ICA adquiriente en un nivel subsidiario, independientemente de que haya una relación de compañía matriz/subsidiaria. Para solicitar el acceso al MOST, un usuario se conecta a MasterCard Connect con su Identificación de Usuario y contraseña, luego solicita al MOST los números de Cliente/ICA específicos de la Tienda de MasterCard Connect.

Luego el pedido se distribuye al Administrador de Seguridad del usuario para su aprobación. Si otra compañía es propietaria de los datos del número de Cliente/ICA, entonces el pedido se distribuye al Administrador de Seguridad de la compañía propietaria de los datos. El Administrador de Seguridad es responsable de aprobar el pedido del usuario del MOST. Después de que los Administradores de Seguridad adecuados aprueban el pedido, el mismo se dirige a MasterCard para su procesamiento. El usuario tiene acceso al MOST después de que MasterCard aprueba el pedido. Los usuarios deben tener una SecurID® de RSA para usar el MOST. Si el usuario no tiene una SecurID [Identificación Segura], se emitirá una como parte del proceso de aprobación para el acceso.

MasterCard rechazará los pedidos del MOST que no están completos y que no son precisos. MasterCard se reserva el derecho de solicitar autorización por escrito de un Contacto de Seguridad del Cliente, Contacto Principal o Contacto del MATCH para validar la solicitud del usuario del MOST. Si MasterCard rechaza un pedido, el usuario debe enviar un pedido posterior para el MOST a través de la Tienda de MasterCard Connect.

Para obtener ayuda adicional con el pedido al MOST, comuníquese con el equipo de Servicios de Operaciones al Cliente utilizando la información de contactos proporcionada en la sección B.6 del Apéndice B.

8.3 Programa de Exceso de Contracargos

MasterCard diseñó el Programa de Exceso de Contracargos (ECP) para motivar a los Adquirientes a controlar, de cerca y continuamente, su desempeño de contracargos a nivel del

Comercio y para determinar lo antes posible cuando un Comercio de MasterCard ha excedido o puede exceder los márgenes mensuales de contracargos.

8.3.1 Definiciones del ECP

Los siguientes términos usados en el ECP tienen el significado establecido a continuación:

Comercio

Un Comercio se define como cualquier establecimiento Comercial identificable de MasterCard, ya sea una ubicación física del Comercio o un sitio de Internet o un localizador uniforme de recursos (URL) del Comercio que el Adquiriente puede identificar por medio de un descriptor de facturación distintivo en el registro de la Transacción.

Relación de los contracargos sobre las transacciones (CTR)

La CTR es el número de contracargos de MasterCard recibidos por el Adquiriente de un Comercio en un mes calendario, dividido por el número de Transacciones de ventas de MasterCard del Comercio realizadas en el mes anterior y adquiridas por dicho Adquiriente. (Una CTR de 1% es igual a 100 puntos base y una CTR de 1,5% es igual a 150 puntos base).

Comercios Controlados por Contracargos (CMM)

Un CMM es un Comercio que posee una CTR de más de 100 puntos base y por lo menos 100 contracargos en un mes calendario.

Comercios con Exceso de Contracargos (ECM)

Un Comercio es un ECM si, en cada uno de dos meses calendario consecutivos (los "meses de activación"), el Comercio tiene una CTR mínima de 150 puntos base y al menos 100 contracargos en cada mes. Esta designación se mantiene hasta que la CTR del ECM esté por debajo de 150 puntos base por un período de dos meses consecutivos.

ECM de Nivel 1

Un Comercio es un ECM de Nivel 1 del primer al sexto mes (consecutivos o no) en que el Comercio es identificado como un ECM.

ECM de Nivel 2

Un Comercio es un ECM de Nivel 2 del séptimo al duodécimo mes (consecutivos o no) en que el Comercio es identificado como un ECM.

8.3.2 Requisitos para la Presentación de Informes

Es responsabilidad del Adquiriente controlar a sus Comercios continuamente, de acuerdo con las Normas, incluyendo, entre otras, las secciones 6.2.2, 7.2, 7.3 y 7.4 de este manual.

El ECP exige al Adquiriente calcular, para cada mes calendario, la CTR en puntos base de cada uno de sus Comercios e informar a MasterCard de cualquier Comercio que sea un CMM o ECM, como se define en la sección 8.3.1.

MasterCard impondrá al Adquiriente de un ECM el cargo por informes descrito en la sección 8.3.2.2.

8.3.2.1 Requisitos para la Presentación de Informes de Comercios Controlados por Contracargos

Cada mes calendario, el Adquiriente debe presentar a MasterCard un informe separado de CMM por cada uno de sus Comercios que califique como un CMM para el mes calendario anterior. Con el fin de determinar si un Adquiriente está obligado a enviar un informe de CMM, el Adquiriente debe calcular la CTR según se establece en la sección 8.3.1. El Adquiriente debe presentar este informe a más tardar 45 días después de la finalización del mes calendario.

El Adquiriente debe enviar el informe de CMM en la forma y manera solicitada por MasterCard. El Adquiriente debe proporcionar también una copia del informe de CMM y estas Normas del ECP al CMM específico.

El Adquiriente debe continuar proporcionando los informes de CMM hasta que el Comercio deje de ser considerado como un CMM durante dos meses consecutivos.

8.3.2.1.1 Contenido del Informe de los CMM

El informe de CMM debe incluir toda la información que se indica a continuación:

- Nombre y ubicación del CMM
- Mes calendario de la calificación CMM que se informa
- CTR del CMM para el mes calendario que se informa
- Código comercial del aceptador de Tarjetas/código de categoría de comercio (MCC) asignados a CMM y una descripción de la naturaleza del negocio del CMM
- Número y volumen bruto en dólares (GDV) de las Transacciones de venta de MasterCard del CMM durante el mes calendario que se informa y durante el mes anterior
- Número y GDV de los contracargos de las Transacciones de venta de MasterCard de CMM durante el mes calendario que se informa
- Cualquier información adicional que MasterCard solicite

8.3.2.1.2 Recargo por Presentación Tardía del Informe de los CMM

Si MasterCard determina que un Comercio es un CMM y el Adquiriente no presenta un informe de CMM a MasterCard en forma oportuna para dicho Comercio, MasterCard puede imponer al Adquiriente un cargo de hasta USD 5.000 por mes por cada mes de retraso de un informe mensual específico de CMM.

8.3.2.2 Requisitos para la Presentación de Informes de Comercios con Exceso de Contracargos

Dentro de los treinta días después de la finalización del segundo mes de activación, y mensualmente a partir de entonces, el Adquiriente debe presentar un informe separado de ECM por cada uno de sus ECM (en lugar de un informe de CMM) hasta que la CTR de ese ECM esté por debajo de 150 puntos base durante dos meses consecutivos. El Adquiriente debe proporcionar también una copia del informe de ECM y estas Normas del ECP al ECM específico. MasterCard impondrá al Adquiriente un cargo por presentación de informes de USD 100 por cada informe de ECM presentado.

El Adquiriente debe continuar proporcionando los informes de ECM mensualmente hasta que el Comercio ya no esté identificado como un ECM durante dos meses consecutivos. Si durante esos meses el Comercio es identificado como un CMM, entonces aplicarán los requisitos de presentación de informes de CMM.

8.3.2.2.1 Contenido del Informe de los ECM

El informe de ECM debe incluir toda la información requerida para el informe del CMM y la información adicional que se detalla a continuación:

- Una descripción de los controles de contracargos del Adquiriente para controlar las actividades del ECM
- Una evaluación de las prácticas que ocasionaron que el ECM excediera las Normas del ECP
- Un plan de acción del Adquiriente para reducir la CTR del ECM
- Un archivo electrónico con los detalles de las Transacciones de contracargo que el Adquiriente recibió para el ECM en el mes calendario
- Cualquier información adicional que MasterCard requiera de vez en cuando

MasterCard impondrá al Adquiriente un cargo por presentación de informes de USD 100 por cada informe de ECM presentado.

8.3.2.2.2 Recargo por Presentación Tardía del Informe de los ECM

Si MasterCard determina que un Comercio es un ECM y el Adquiriente no presenta a MasterCard un informe de ECM en forma oportuna para dicho ECM, MasterCard puede imponer al Adquiriente un cargo de hasta USD 500 por día por cada uno de los primeros 15 días de retraso del informe de ECM para dicho ECM y hasta USD 1.000 por día, de ahí en adelante, hasta que se presente el informe de ECM demorado.

8.3.3 Recargos

Además de los recargos correspondientes a los informes de ECM o a las presentaciones tardías de informes, MasterCard puede imponer al Adquiriente cargos por violación y reembolso del Emisor por el exceso de contracargos que surja de un ECM. MasterCard calcula los cargos y recargos por reembolso del Emisor según se describe en la sección 8.3.3.1 y se aplican en cada mes calendario en que el ECM excede una CTR de 150 puntos base después del primer mes de activación. Con el fin de calcular los cargos y recargos por reembolso del Emisor (y no con el propósito de satisfacer los requisitos de presentación de informes contenidos en este documento), un Adquiriente puede ofrecer un cálculo de CTR alternativo que "relacione" o enlace los contracargos con más exactitud a las Transacciones de ventas pertinentes.

Durante los primeros 12 meses de la identificación de un Comercio como ECM, MasterCard tendrá en cuenta el volumen real de contracargos del Comercio en el momento de determinar la responsabilidad del Adquiriente. Durante este período, MasterCard impondrá un cargo al Adquiriente, el menor de:

- El total del reembolso del Emisor más montos de recargo por violación, calculado según se describe en la sección 8.3.3.1, en un mes determinado, o
- El volumen en dólares de contracargos del Comercio comunicados por el Adquiriente para ese mes.

8.3.3.1 ECP Assessment Calculation

MasterCard determines an Acquirer's liability for the monthly Issuer reimbursement fees and assessments for each ECM as set forth below. MasterCard calculates the Issuer reimbursement fees in the following Steps 1, 2, and 3, and calculates the violation assessment in Step 4.

1. Calculate the CTR for each calendar month that the ECM exceeded a CTR of 150 basis points (which may also be expressed as 1.5% or 0.015).
2. From the total number of chargebacks in the above CTR calculation, subtract the number of chargebacks that account for the first 150 basis points of the CTR. (This amount is equivalent to 1.5 percent of the number of monthly sales Transactions used to calculate the CTR.) The result is the number of chargebacks above the threshold of 150 basis points.
3. Multiply the result from Step 2 by USD 25. This is the Issuer reimbursement.
4. Adjust the result in Step 3 to reflect the extent that the Acquirer has exceeded the 150 basis points threshold by multiplying the value in Step 3 by the CTR (expressed as basis points). Divide this result by 100. This amount is the violation assessment.

Repeat Steps 1–4 for each calendar month (other than the first trigger month) that the ECM exceeded a CTR of 150 basis points or 1.5 percent.

Example: The Acquirer for Merchant ABC acquired MasterCard sales Transactions and chargebacks over a six-month period as follows:

Month	January	February	March	April	May	June	July
Sales Transactions	95,665	95,460	95,561	95,867	95,255	95,889	95,758
Chargebacks	1,050	1,467	1,635	1,556	1,495	1,052	985
CTR in basis points	—	153	171	163	156	110	103

February and March are the trigger months, as these are two consecutive months where the CTR exceeded 150 basis points. At the end of July, Merchant ABC was no longer an ECM as its CTR was below 150 basis points for two consecutive months. MasterCard calculates assessments and Issuer reimbursements for each of the months March through July.

For example, the assessment for April (using March sales Transactions and April chargeback volumes) is calculated as follows:

- The CTR = April chargebacks/March sales Transactions = 1,556/95,561 = 0.01628 or 163 basis points (rounded)
- The number of chargebacks in excess of the 150 basis points is determined by subtracting 1.5 percent of the March sales Transactions from the number of April chargebacks. 1.5 percent of the March sales Transactions (95,561 x 0.015) is 1,433. 1,556 – 1,433 = 123 chargebacks

- The Issuer reimbursement for April is 123 x USD 25 = USD 3,075
- The violation assessment is (USD 3,075 x 163)/100 or 501,225/100 = USD 5,012.25

Using this methodology, the Issuer reimbursement fees and assessments for the Acquirer for Merchant ABC are as follows.

Month	Issuer Reimbursement	Assessment	Total
February (first trigger month)	0	0	0
March (second trigger month)	USD 5,075.00	USD 8,678.25	USD 13,753.25
April	USD 3,075.00	USD 5,012.25	USD 8,087.25
May	USD 1,425.00	USD 2,223.00	USD 3,648.00
June	0	0	0
July	0	0	0
Total	USD 9,575.00	USD 15,913.50	USD 25,488.50

Example: For the month of March, the Acquirer reported Merchant ABC chargeback volume of 1,635 chargebacks totaling USD 12,145. This amount is less than the calculated amount of the Issuer reimbursement plus violation assessment total of USD 13,753.25, as shown above for March. Therefore, MasterCard will assess the Acquirer the lesser chargeback volume amount rather than the greater calculated amount.

8.3.4 Reembolso del Emisor

MasterCard enviará los cargos por reembolso del Emisor a través del MCBS. Los reembolsos reales variarán dependiendo del alcance y la duración de la infracción y del número de contracargos procesados por cada Emisor, y se pagarán de los montos cobrados por los cargos por reembolso del Emisor descritos en la sección 8.3.3.1 en forma prorrateada.

8.3.5 Additional Tier 2 ECM Requirements

After a Merchant has been a Tier 1 ECM for six months (whether consecutive or non-consecutive), the Merchant will be deemed a Tier 2 ECM in its seventh month as an ECM.

With respect to a Tier 2 ECM, MasterCard may:

1. Advise the Acquirer with regard to the action plan and other measures that the Acquirer should take or consider taking to reduce the Merchant's CTR; and/or

2. Require the Acquirer to undergo a Global Risk Management Program Customer Risk Review, at the Acquirer's expense, as described in Chapter 13 of this manual.

After a Merchant has been an ECM for 12 months (whether consecutive or non-consecutive), the Acquirer will be deemed to be in violation of Rule 5.11.7 of the *MasterCard Rules* manual ("the Illegal or Brand-damaging Transactions Rule"), and in addition to the assessments described in section 8.3.3, is subject to noncompliance assessments of up to USD 50,000 per month after the twelfth month that the Merchant remains an ECM.

8.4 Programa de Auditoría al Comercio Sospechoso (QMAP)

El Programa de Auditoría del Comercio Sospechoso (QMAP) establece las normas mínimas del comportamiento aceptable del Comercio e identifica a los Comercios que podrían no cumplir con dichas normas mínimas al participar en actividad inapropiada o de otro modo, fraudulenta o de confabulación. El QMAP también permite que un Emisor obtenga una recuperación parcial de hasta la mitad de las pérdidas por fraude reales resultantes de transacciones fraudulentas en un Comercio Sospechoso, de acuerdo con los informes del SAFE. Los criterios para identificar a un Comercio Sospechoso y el proceso de recuperación por fraude se describen a continuación.

8.4.1 QMAP Definitions

For purposes of the QMAP, the following terms have the meanings set forth below:

Cardholder bust-out account means an account for which all of the following conditions are true:

1. The Issuer closed the account prior to the earlier of (i) the Issuer requesting that MasterCard commence an investigation as to whether a Merchant is a Questionable Merchant, or (ii) MasterCard notifying the Issuer that MasterCard has commenced an investigation as to whether a Merchant is a Questionable Merchant; and
2. A Transaction arising from use of the account has not been charged back for either an authorization-related chargeback (as set forth in section 3.2 of the *Chargeback Guide*) or fraud-related chargeback (as set forth in section 3.3 of the *Chargeback Guide*) during the 180 days prior to the earlier of (i) the Issuer requesting that MasterCard commence an investigation as to whether a Merchant is a Questionable Merchant, or (ii) MasterCard notifying the Issuer that MasterCard has commenced an investigation as to whether a Merchant is a Questionable Merchant; and
3. At least one of the following is true:

    a. The account in question is "linked" to one or more Cardholder bust-out accounts. As used herein, to be "linked" means that personal, non-public information previously provided by an applicant in connection with the establishment of one or more Cardholder bust-out accounts (name, address, telephone number, social security number or other government-issued identification number, authorized user, demand deposit account number, and the like) has been provided by an applicant in connection with the establishment of the subject account; or

b. The account is linked to one or more Cardholder bust-out accounts used in Transactions with a Merchant that MasterCard identified as a Questionable Merchant in a *Global Security Bulletin*; or
c. The Cardholder requests that one or more additional persons be designated as an additional Cardholder of the account within a short period of time; or
d. The Cardholder requests that the credit limit of the account be increased soon after the account is opened; or
e. The Cardholder makes frequent balance queries or "open-to-buy" queries; or
f. No payment has been made of charges to the account; or
g. The Issuer closed the account after a failed payment (dishonored check or the like) of charges to the account.

Case Scope Period means the 180-calendar-day period preceding the date on which MasterCard commences an investigation into the activities of a suspected Questionable Merchant.

Questionable Merchant means a Merchant that satisfies all of the following criteria:

1. The Merchant submitted at least USD 50,000 in Transaction volume during the Case Scope Period;
2. The Merchant submitted at least five (5) Transactions to one or more Acquirers during the Case Scope Period; and
3. At least fifty (50) percent of the Merchant's total Transaction volume involved the use of Cardholder bust-out accounts

   OR

   At least three (3) of the following four (4) conditions apply to the Merchant's Transaction activity during the Case Scope Period:

   a. The Merchant's fraud-to-sales Transaction ratio was seventy (70) percent or greater.
   b. At least twenty (20) percent of the Merchant's Transactions submitted for authorization were declined by the Issuer or received a response of "01—Refer to issuer" during the Case Scope Period.
   c. The Merchant has been submitting Transactions for fewer than six (6) months.
   d. The Merchant's total number or total dollar amount of fraudulent Transactions, authorization declines, and Issuer referrals was greater than the Merchant's total number or total dollar amount of approved Transactions.

NOTA: Transaction activity ("on-us" or otherwise) that is not processed through MasterCard systems is not considered in determining whether a Merchant meets the criteria of a Questionable Merchant.

MasterCard has sole discretion, based on information from any source, to determine whether a Merchant meeting these criteria is a Questionable Merchant.

8.4.2 MasterCard Commencement of an Investigation

MasterCard, at its sole discretion, may commence a QMAP investigation of a Merchant. During the pendency of such an investigation, MasterCard may identify the Merchant being investigated in MATCH using MATCH reason code 00 (Questionable Merchant/Under Investigation).

If an Issuer has reason to believe that a Merchant may be a Questionable Merchant, the Issuer must promptly notify MasterCard via email message at qmap@mastercard.com. Transactions that occurred during the Case Scope Period may qualify as eligible for recovery under the QMAP.

In the notification, the Issuer must provide the basis for the Issuer's reason to believe that the Merchant may be a Questionable Merchant, and must provide all of the following information:

1. Issuer name and Member ID;
2. Acquirer name and Member ID;
3. Merchant name and address (city, state or province, and country);
4. Total number of Transactions conducted at the Questionable Merchant by the Issuer's Cardholders;
5. Total dollar volume of Issuer losses at the Questionable Merchant;
6. Percentage of Transactions attributed to Cardholder bust-out accounts, if applicable; and
7. Details of each Issuer-confirmed fraudulent Transaction, including Cardholder account number, Transaction date and time, and Transaction amount in U.S. dollars.

If an Acquirer becomes aware that it is acquiring for a Questionable Merchant, the Acquirer must notify MasterCard promptly via email message at qmap@mastercard.com.

8.4.3 Notificación de MasterCard a los Emisores

MasterCard notificará a los Emisores afectados sobre el comienzo de una investigación del QMAP de un Comercio según se indica a continuación, dependiendo de si la investigación involucra cuentas bust-out del Tarjetahabiente.

8.4.3.1 Investigations Concerning Cardholder Bust-out Accounts

If MasterCard commences a QMAP investigation concerning Cardholder bust-out accounts, MasterCard will notify an Issuer that MasterCard determines had accounts used in Transactions with the Merchant being investigated during the Case Scope Period.

The notification will be sent via email message to the Issuer's Security Contact then listed in the Member Information—MasterCard application available on MasterCard Connect. With the notification, MasterCard will provide details of Transactions arising from use of the Issuer's accounts at the Merchant during the Case Scope Period.

Within 60 days following such notice, an Issuer must report to SAFE all fraudulent Transactions conducted during the Case Scope Period associated with the Merchant being investigated. Transactions conducted on Cardholder bust-out accounts should be reported using fraud type code 51 (Bust-out Collusive Merchant).

NOTA: To accelerate the determination by MasterCard of whether a Merchant is a Questionable Merchant, Issuers are urged to report fraudulent Transactions to SAFE as expeditiously as feasible. For purposes of making such a determination, MasterCard only considers Transactions that take place (and the resulting fraudulent Transactions timely reported to SAFE) during the Case Scope Period.

8.4.3.2 Investigations Not Concerning Cardholder Bust-out Accounts

If MasterCard commences a QMAP investigation not concerning Cardholder bust-out accounts, MasterCard will notify an Issuer that MasterCard determines had accounts used in Transactions with the Merchant being investigated during the Case Scope Period only if MasterCard determines that the Merchant is a Questionable Merchant.

The notification will be sent via email message to the Issuer's Security Contact then listed in the Member Information—MasterCard application available on MasterCard Connect.

8.4.4 MasterCard Notification to Acquirers

Following the MasterCard evaluation of Transactions reported to SAFE by Issuers, MasterCard may notify any Acquirer of the investigated Merchant that such Merchant has initially met the criteria of a Questionable Merchant. Such notification will be sent via email message to the Security Contact then listed for the Acquirer in the Member Information—MasterCard application available on MasterCard Connect.

Within 15 calendar days from the date of the MasterCard notification, the Acquirer may contest the MasterCard preliminary finding that a Merchant is a Questionable Merchant. In such an event, the Acquirer shall provide to MasterCard any supplemental information necessary to review the preliminary finding.

MasterCard has a right, but not an obligation, to audit an Acquirer's records for the purpose of attempting to determine whether a Merchant is a Questionable Merchant. An Acquirer must provide MasterCard such other or additional information as MasterCard may request to assist in the investigation.

The Acquirer must submit all documentation and records via email message to qmap@mastercard.com.

8.4.5 Cancelación del Comercio

Si el Adquiriente determina que el Comercio bajo investigación (u otro de sus Comercios) es un Comercio Sospechoso y rescinde el Convenio de Comercio por dicho motivo, el Adquiriente debe agregar al Comercio en MATCH usando el código de motivo 08 de MATCH (Programa de Auditoría del Comercio Sospechoso de MasterCard) dentro de los cinco (5) días calendario de la decisión para rescindir al Comercio.

8.4.6 MasterCard Determination

MasterCard will determine if a Merchant is a Questionable Merchant.

If MasterCard determines that the Merchant **is not** a Questionable Merchant, MasterCard will so notify each Issuer and Acquirer that provided information pertinent to the investigation.

Such notice will be provided via email message to the Security Contact listed for the Customer in the Member Information—MasterCard application available on MasterCard Connect. In addition, MasterCard will delete the MATCH listing of the Merchant for MATCH reason code 00.

If MasterCard determines that the Merchant **is** a Questionable Merchant, MasterCard will:

1. Notify the Merchant's Acquirer, and
2. Identify the Merchant as a Questionable Merchant in a *Global Security Bulletin* for each of twelve (12) consecutive months, and
3. Modify the Merchant's MATCH record to reflect a reason code change from 00 (Under Investigation) to 20 (MasterCard Questionable Merchant Audit Program).

If the Acquirer terminates the Merchant Agreement because MasterCard determines the Merchant to be a Questionable Merchant, the Acquirer is required to identify the Merchant in MATCH with reason code 08 (MasterCard Questionable Merchant Audit Program).

8.4.7 Responsabilidad del Contracargo

Cuando MasterCard identifica a un Comercio Sospechoso en un *Boletín de Seguridad Global*, MasterCard también especificará un período de contracargo (fechas de "inicio" y "fin") de al menos un año. Si un Adquiriente continúa adquiriendo de un Comercio luego de que MasterCard declara al Comercio como Comercio Sospechoso, el Adquiriente es responsable de los contracargos válidos usando el código de motivo de mensaje 4849—Actividad Sospechosa del Comercio por un período de un año después de la publicación del *Boletín de Seguridad Global* que inicialmente lista al Comercio Sospechoso; siempre y cuando MasterCard pueda extender el período de responsabilidad del contracargo. Un Emisor tiene 120 días luego de la fecha de publicación de un *Boletín de Seguridad Global* que identifica a un Comercio Sospechoso para contracargar al Adquiriente Transacciones fraudulentas que se lleven a cabo durante el período especificado de contracargo usando el código de motivo 4849—Actividad Sospechosa del Comercio.

8.4.8 Recuperación por Fraude

Tras la identificación de un Comercio Sospechoso en un *Boletín de Seguridad Global*, y utilizando los datos informados al SAFE, MasterCard notificará a todo Emisor que MasterCard considere elegible para la recuperación parcial de la pérdida debido a Transacciones fraudulentas en un Comercio Sospechoso. La notificación divulgará el monto de la recuperación, menos un cargo administrativo descrito en la sección 8.4.9, y la fecha en que el monto se acreditará en la cuenta del MCBS del Emisor.

Un Emisor no es elegible para recibir la recuperación parcial de cualquier Transacción:

1. De un Comercio no listado en el *Boletín de Seguridad Global*, o
2. Que tenga lugar después de la fecha de publicación del *Boletín de Seguridad Global*, o
3. No informado a MasterCard por medio de SAFE según se describe en la sección 8.4.3 de este manual, o

4. Para el cual el Emisor recibió la recuperación por medio de cualquier resarcimiento existente en el sistema de MasterCard, incluyendo contracargos, proceso de recuperación, o el proceso de cobro propio del Emisor.

MasterCard se reserva el derecho de solicitar información adicional como una condición para determinar si una Transacción cumple, de forma satisfactoria, con los requisitos de elegibilidad para la recuperación parcial del Emisor. Además, MasterCard no pagará el excedente cuando la reclamación sea mayor al monto cobrado del Adquiriente por ese propósito.

MasterCard debitará el monto de recuperación por fraude de la cuenta del Adquiriente y lo acreditará en la cuenta del Emisor (menos cualquier cargo administrativo). MasterCard procesará las recuperaciones por fraude del Emisor por medio del MCBS.

8.4.9 Cargos del QMAP

MasterCard puede cobrarle a cada Emisor un cargo administrativo igual al 10 por ciento del monto de recuperación del Emisor a partir de una determinación de Comercio Sospechoso.

MasterCard puede cobrarle a un Adquiriente un costo de auditoría que no exceda USD 2.500 para cada identificación de un Comercio como un Comercio Sospechoso.

8.5 Programa de Control del Emisor (IMP)

MasterCard diseñó el Programa de Control del Emisor (IMP) para alentar a cada Emisor a controlar de cerca y de forma continua su desempeño con respecto a las tasas de rechazo de fraude, contracargos y autorizaciones a fin de determinar cuándo el Emisor ha sobrepasado o posiblemente sobrepase los márgenes trimestrales de rechazo de autorización de las Transacciones Transfronterizas, pérdidas por fraude y contracargos relacionados con fraude.

8.5.1 Criterios de Identificación

MasterCard analizará las mediciones trimestrales relacionadas con los rechazos de autorizaciones de Transacciones Transfronterizas, contracargos relacionados con fraude y pérdidas por fraude con el fin de identificar un Emisor en el IMP. MasterCard exigirá al Emisor que participe en una auditoria del IMP si se cumple alguno de los criterios siguientes:

1. El Emisor comunicó al menos USD 100.000 en pérdidas por fraude por trimestre al SAFE, que representan al menos tres veces el promedio bruto de puntos base de fraude a MasterCard del país; **o**
2. El Emisor rechazó al menos el sesenta (60) por ciento de sus Transacciones Internacionales presentadas para su autorización durante el trimestre; **o**
3. El Emisor posee cinco (5) o más números de cuenta primarios (PAN) en los cuales el Emisor inició al menos treinta y cinco (35) contracargos por PAN relacionados con fraude, **y** dichos PAN representan al menos el dos (2) por ciento del número total de PAN en los cuales el Emisor contracargó al menos una Transacción fraudulenta.

NOTA:

De vez en cuando, MasterCard alineará el número de contracargos relacionados con fraude utilizados por el IMP con el número de contracargos relacionados con fraude utilizados por el contador del Servicio de Notificación de Fraude (FNS).

Para el tercer criterio solamente, la identificación en el IMP estará basada en las Transacciones con Tarjetas MasterCard®, Maestro® y Cirrus®, a fin de alinearlas con el contador del FNS. Para el primer y segundo criterio, la identificación en el IMP estará basada en las Transacciones con Tarjetas MasterCard solamente. Las Transacciones con Tarjetas Maestro y Cirrus no se incluirán.

8.5.2 Auditoría y Cuestionario de MasterCard

MasterCard comenzará una auditoría del IMP si un Emisor cumple o sobrepasa al menos uno de los criterios de identificación del IMP enumerados en la sección 8.5.1. MasterCard continuará con la auditoría del IMP, a menos que MasterCard conceda una exclusión o hasta que el Emisor permanezca por debajo de los criterios de identificación del IMP por dos (2) trimestres consecutivos.

Al comienzo de la auditoría del IMP, MasterCard notificará al Emisor identificado sobre dicha decisión. Al momento de la notificación, MasterCard proporcionará también al Emisor un cuestionario relativo al programa de control de pérdidas por fraude del Emisor.

Dentro de 30 días calendario a partir de la fecha de la notificación de MasterCard, el Emisor debe presentar a MasterCard respuestas completas y precisas al cuestionario y proporcionar ejemplos de informes diarios de control de fraude. En el cuestionario, el Emisor puede informar también sobre cualquier circunstancia atenuante (incluyendo, entre otras, un Evento de Compromiso de los Datos de la Cuenta [ADC]) que demuestre por qué los resultados de dicho trimestre resultaron anómalos. MasterCard considerará dicha información a fin de determinar si concede una exclusión para dicho trimestre.

8.5.3 Subsequent Issuer Identifications in the IMP

Upon determination by MasterCard of the Issuer's required participation in the IMP audit, the Issuer must take reasonable steps to improve its fraud loss control program.

If the Issuer's Activity meets or exceeds the identification criteria as set forth in section 8.5.1 for a second time within a given 12-month period (that is, the Issuer's second IMP identification), the Issuer must provide to MasterCard a detailed action plan describing the steps that the Issuer will take to improve its fraud management and risk mitigation performance. MasterCard also reserves the right to require the Issuer to undergo a Global Risk Management Program Customer Risk Review.

For all subsequent identifications of the Issuer in the IMP, the Issuer may be subject to the following quarterly assessments.

Quarterly Assessment Description	Assessment Amount
Third IMP Identification	USD 25,000
Fourth IMP Identification	USD 50,000
Each Subsequent IMP Identification	USD 100,000

Capítulo 9 Programa de Inscripción a MasterCard

Este capítulo puede ser de interés especial para el personal del Cliente responsable de inscribir a los Comercios, Comercios Secundarios, y otras entidades con MasterCard. El Programa de Inscripción en MasterCard (MRP) anteriormente era conocido como el Programa de Inscripción del Comercio.

9.1 Generalidades del Programa de Inscripción a MasterCard

MasterCard requiere que los Clientes inscriban los siguientes tipos de Comercios, incluyendo los Comercios Secundarios y otras entidades por medio del sistema del Programa de Inscripción de MasterCard (MRP), disponible a través de MasterCard Connect™:

- Comercios de contenido y servicios para adultos que no son cara a cara—MCC 5967 y 7841 (consulte la sección 9.4.1)
- Comercios de juegos de azar que no son cara a cara—MCC 7801, 7802 y 7995 (consulte la sección 9.4.2)
- Comercios farmacéuticos que no son cara a cara—MCC 5122 y MCC 5912 (consulte la sección 9.4.3)
- Comercios de productos de tabaco que no son cara a cara—MCC 5993 (consulte la sección 9.4.3)
- Comercios de lotería gubernamental (Región de EE. UU. solamente)—MCC 7800 (consulte la sección 9.4.4)
- Comercios de lotería gubernamental (países específicos)—MCC 9406 (consulte la sección 9.4.4)
- Comercios de juegos de habilidades (Región de EE. UU. solamente)—MCC 7994 (consulte la sección 9.4.5)

  Para un Comercio de juegos de habilidades, el Cliente debe presentar la solicitud de inscripción a MasterCard enviando un correo electrónico a mrp@mastercard.com.
- Comercios de cyberlocker de alto riesgo—MCC 4816 (consulte la sección 9.4.6)
- Comercios informados bajo el Programa de Exceso de Contracargos (consulte la sección 8.3)

Durante la inscripción, el Adquiriente debe proporcionar cada localizador de recursos uniforme (URL) de sitio web desde el cual pueden surgir las Transacciones, según se describe en esta sección, tanto si el sitio web es de un Comercio, Comercio Secundario de un Facilitador de Pagos o de otra entidad. Con respecto a las Transacciones presentadas por un Operador de Billetera Digital por Etapas (DWO), se deben inscribir en forma individual todos los URL de sitio web individuales en los cuales se pueden efectuar Transacciones según se describe en esta sección.

Si un Cliente adquiere Transacciones para cualquiera de los tipos de Comercios listados en el presente sin inscripción previa del Comercio o Comercio Secundario conforme a las Normas descritas en esta sección, MasterCard podrá imponer un cargo al Cliente, según se estipula en la sección 9.2.1 de este manual. Además, el Adquiriente debe asegurarse de que la infracción se corrija rápidamente.

Consulte el *MasterCard Registration Program User Manual* para obtener las instrucciones para completar las tareas de inscripción disponibles en el sistema MRP.

9.2 Requisitos Generales de Inscripción

El Cliente debe proporcionar toda la información solicitada por cada Comercio, Comercio Secundario, u otra entidad que deba inscribirse a través del sistema del MRP. Para cada entidad, la información solicitada incluye:

- Nombre, nombre bajo el cual opera el comercio (DBA) y dirección
- Número de teléfono central de acceso, o número de teléfono del servicio al cliente, URL del sitio web, o dirección de correo electrónico
- Nombre/s, dirección/es y número/s de identificación tributaria (u otro número de identificación nacional pertinente) del/los propietario/s principal/es
- Una descripción detallada del(de los) servicio(s), producto(s), o de ambos, que la entidad ofrecerá a los Tarjetahabientes
- Una descripción de los procedimientos del procesamiento de pago, las divulgaciones del Tarjetahabiente y otras prácticas que incluyen, entre otras:
  - Datos solicitados del Tarjetahabiente
  - Proceso de autorización (incluyendo los límites de piso)
  - Políticas de devolución del departamento de servicio al cliente de las transacciones de tarjetas
  - Divulgación por parte del Comercio antes de solicitar la información de pago (incluyendo la conversión de moneda en el Punto de Interacción [POI])
  - Prácticas de almacenamiento y seguridad de los datos
- Identidad de cualquier relación(es) comercial anterior que involucre al(a los) propietario(s) principal(es) de la entidad
- Una certificación del funcionario del Cliente, responsable directo de asegurar el acatamiento de la entidad inscrita a las Normas, declarando que después de haber llevado a cabo una investigación diligente y de buena fe, el Cliente cree que la información que aparece en la solicitud de inscripción es verdadera y precisa

Solamente MasterCard puede modificar o eliminar la información sobre una entidad inscrita. Los clientes deben presentar por escrito a MasterCard cualquier modificación a una entidad inscrita, explicando el motivo de la solicitud. MasterCard se reserva el derecho de rechazar una solicitud de modificación.

Los clientes deberán enviar la información solicitada y las solicitudes de modificación adicionales al vicepresidente de Control de Fraude del Comercio, a la dirección proporcionada en el Apéndice B.

Para conocer los requisitos específicos de los Comercios que deben implementar el Programa de Protección de los Datos del Sitio (SDP) de MasterCard, consulte la sección 10.3 de este manual.

9.2.1 Merchant Registration Fees and Noncompliance Assessments

MasterCard assesses the Acquirer an annual USD 500 registration fee for each Merchant and Submerchant under the categories listed in section 9.1, except Merchants reported under the

Excessive Chargeback Program. MasterCard will collect the fee from the Acquirer via the MasterCard Consolidated Billing System (MCBS).

MasterCard may assess a Customer that acquires Transactions for any of these Merchant or Submerchant types without first registering the Merchant in accordance with the requirements of the MRP. A violation will result in an assessment of up to USD 10,000.

If, after notice by MasterCard of the Acquirer's failure to register a Merchant or Submerchant, that Acquirer fails to register its Merchant within 10 days of notice, the Acquirer will be subject to additional assessments of USD 5,000 per month for up to three months, and USD 25,000 per month thereafter, until the Acquirer satisfies the requirement. In addition, the Acquirer must ensure that the violation is corrected promptly. Such Merchant or Submerchant may also be deemed by MasterCard, in its sole discretion, to be in violation of Rule 5.11.7 of the *MasterCard Rules* manual ("the Illegal or Brand-damaging Transactions Rule").

9.3 Requisitos Generales de Control

Los requisitos de control descritos en esta sección aplican a los Clientes que adquieren Transacciones de contenido y servicios para adultos que no son cara a cara, Transacciones de juegos de azar que no son cara a cara, Transacciones de productos farmacéuticos y tabaco que no son cara a cara, Transacciones de lotería gubernamental, Transacciones de juegos de habilidad (Región de EE. UU. solamente), Transacciones de cyberlocker de alto riesgo, o Transacciones de Comercios informados bajo el Programa de Exceso de Contracargos:

- Además, el Adquiriente debe asegurarse de que cada Comercio implemente los procedimientos en tiempo real y de grupo de transacciones para controlar continuamente todo lo siguiente:
  - Múltiples Transacciones simultáneas que utilizan el mismo número de Cuenta
  - Intentos consecutivos o excesivos con el mismo número de Cuenta

  Cuando el intento de fraude es evidente, el Comercio debe implementar el bloqueo temporal del número de identificación bancaria (BIN) para evitar el fraude.
- El Adquiriente debe asegurarse de que cada Comercio acate las Normas de control de fraude especificadas en el Capítulo 6 de este manual y que mantenga un índice total de volumen de contracargos sobre ventas de intercambio por debajo de los márgenes del Programa de Exceso de Contracargos. Para obtener información sobre el Programa de Exceso de Contracargos, consulte la sección 8.3 de este manual.

9.4 Requisitos Adicionales para Categorías de Comercios Específicas

Los clientes deben revisar cuidadosamente estos requisitos adicionales para las categorías de Comercio específicas.

9.4.1 Comercios de Contenido y Servicios para Adultos que No son Cara a Cara

Una Transacción de contenido y servicios para adultos que no es cara a cara se lleva a cabo cuando un consumidor utiliza una Cuenta en un entorno sin Tarjeta presente para comprar contenido o servicios para adultos, que puede incluir, entre otros, acceso a un sitio web por suscripción; transmisión de video; y alquiler y venta de DVD y cintas de video.

Un Adquiriente debe identificar todas las Transacciones de contenido y servicios para adultos que no son cara a cara usando una de las siguientes combinaciones de MCC y TCC, según corresponda:

- MCC 5967 (Mercadeo Directo—Comercios de Telemercadeo Entrante) y TCC T; o
- MCC 7841 (Tiendas de Alquiler de Videos de Entretenimiento) y TCC T.

Antes de que un Adquiriente pueda procesar Transacciones de contenido y servicios para adultos que no son cara a cara de un Comercio o un Comercio Secundario, debe inscribir al Comercio en MasterCard según se describe en la sección 9.2 de este manual.

9.4.2 Comercios de Juegos de Azar que No son Cara a Cara

Una Transacción de juegos de azar que no es cara a cara tiene lugar en un entorno Sin Presencia de Tarjeta cuando un consumidor usa una Cuenta para hacer una apuesta o comprar fichas de juego u otros valores que se pueden usar para juegos de azar, proporcionados por un establecimiento de apuestas según lo define el MCC 7801 (Juegos de Azar por Internet), MCC 7802 (Carreras de Caballos/Galgos con Licencia del Gobierno) o el MCC 7995 (Transacciones de Juegos de Azar).

Antes de adquirir Transacciones que reflejen juegos de azar que no son cara a cara, el Adquiriente debe inscribir primero al Comercio o Comercio Secundario con MasterCard según se describe en la sección 9.2.

Un Adquiriente debe identificar todas las Transacciones de juegos de azar que no son cara a cara usando el MCC 7995 y el TCC U, a menos que el Adquiriente haya inscrito también al Comercio o Comercio Secundario, según se describe a continuación, en cuyo caso el Adquiriente podrá usar el MCC 7801 ó 7802 en lugar del MCC 7995.

Además de los requisitos de inscripción del Comercio o Comercio Secundario, según se describe en la sección 9.2, un Adquiriente de la Región de EE. UU. que inscribe a un Comercio o Comercio Secundario de la Región de EE. UU. que participa en actividades legales de juegos de azar que involucran carreras de caballos, carreras de galgos o juegos de azar por Internet Intraestatales que no son deportivos debe demostrar que se efectuó una revisión de diligencia debida adecuada, proporcionando los siguientes elementos a MasterCard como parte del proceso de inscripción (en el presente documento, todas las referencias a un Comercio también aplican a un Comercio Secundario):

1. **Evidencia de la autoridad legal.** El Adquiriente debe proporcionar:
   - una copia de la licencia del Comercio (o documento similar), si existe, emitida por la autoridad gubernamental adecuada (por ejemplo el estado o tribu), que autorice claramente al Comercio para participar en actividades de juegos de azar; y

- cualquier ley aplicable al Comercio que permita que se efectúe la actividad de juegos de azar.

2. **Opinión legal.** El Adquiriente debe obtener una opinión legal justificada, dirigida al Adquiriente, de un abogado de EE. UU. o firma legal de EE. UU. del sector privado. La opinión legal debe:

   - identificar todas las leyes de juegos de azar, juegos y leyes similares correspondientes aplicables al Comercio;
   - identificar todas las leyes de juegos de azar, juegos y leyes similares correspondientes aplicables a los Tarjetahabientes a quienes el Comercio permite efectuar transacciones con el Comercio; y
   - demostrar que los juegos de azar y las actividades de pago del Comercio y de los Tarjetahabientes acatan en todo momento las leyes identificadas anteriormente.

   El Adquiriente debe proporcionar a MasterCard una copia de dicha opinión legal. La opinión legal debe ser aceptable para MasterCard a su entera discreción.
3. **Controles eficaces.** El Adquiriente debe proporcionar la certificación de un tercero independiente calificado que demuestre que los sistemas del Comercio para las operaciones de su negocio de juegos de azar:

   - incluyen la verificación eficaz de la edad y ubicación; y
   - están diseñados razonablemente para garantizar que el negocio de juegos de azar por Internet del Comercio permanecerá dentro de los límites legales (incluyendo las leyes relacionadas con Transacciones interestatales).

   La certificación debe incluir todas las capturas de pantalla pertinentes a la certificación (por ejemplo, el proceso de verificación de la edad). Las certificaciones de las partes interesadas (tales como el Adquiriente, las Organizaciones de Ventas Independientes [ISO], el Comercio, etcétera) no son sustitutos aceptables de la certificación de un tercero independiente.
4. **Notificación de cambios.** El Adquiriente debe certificar que notificará a MasterCard sobre cualquier cambio a la información que ha proporcionado a MasterCard, incluyendo los cambios a las leyes correspondientes, las actividades del Comercio y los sistemas del Comercio. Dicha notificación debe incluir cualquier revisión o adición a la información proporcionada a MasterCard (por ejemplo, la opinión legal, la certificación de terceros) para actualizar y completar la información. Dicha notificación se debe proporcionar dentro de los primeros diez (10) días a partir de que se efectuó el cambio.
5. **Aceptación de las responsabilidades.** El Adquiriente debe afirmar específicamente que no presentará Transacciones restringidas del Comercio para la autorización. El Adquiriente también debe reafirmar específicamente su indemnización a MasterCard en conexión con las actividades del Adquiriente o del Comercio. Dicha reafirmación deberá indicar específicamente que el Adquiriente reconoce y acepta que las Transacciones constituyen la Actividad del Adquiriente y que están sujetas a la Regla 2.3 del manual *Reglamento de MasterCard*, independientemente del acatamiento del Adquiriente con la *Política de Juegos de Azar por Internet* de MasterCard o con estos requisitos.

9.4.3 Comercios de Productos Farmacéuticos y de Tabaco

Una Transacción de productos farmacéuticos que no es cara a cara tiene lugar en un entorno Sin tarjeta presente cuando un consumidor usa una Cuenta para comprar medicamentos con receta de un Comercio cuyo negocio principal es vender medicamentos con receta por medio de una transacción que no es cara a cara.

Una Transacción de productos de tabaco que no es cara a cara tiene lugar en un entorno Sin tarjeta presente cuando un consumidor usa una Cuenta para comprar productos de tabaco (incluyendo, entre otros, cigarrillos, cigarros o tabaco suelto) de un Comercio cuyo negocio principal es vender productos de tabaco por medio de una transacción que no es cara a cara.

Antes de adquirir las Transacciones descritas a continuación, un Adquiriente debe inscribir primero al Comercio con MasterCard según se describe en la sección 9.2:

- Venta de productos farmacéuticos que no es cara a cara (MCC 5122 y MCC 5912)
- Venta de productos de tabaco que no es cara a cara (MCC 5993)

Un Adquiriente debe identificar todas las Transacciones de productos farmacéuticos que no son cara a cara, usando el MCC 5122 (Medicamentos, Propietarios de Medicamentos Patentados y Artículos Diversos de Farmacia) y el TCC T para las compras al por mayor o el MCC 5912 (Droguerías, Farmacias) y el TCC T para las compras al por menor. Un Adquiriente debe identificar todas las Transacciones de productos de tabaco que no son cara a cara usando el MCC 5993 (Tiendas y Expendedores de Tabaco) y el TCC T.

Con fines de aclaración, el término adquisición, según se usa en esta sección, se refiere a "Actividad de adquisición", según se usa dicho término en la Regla 2.3 del manual *Reglamento de MasterCard*.

En el momento de inscribir a un Comercio o Comercio Secundario de acuerdo con esta sección, el Adquiriente de dicho Comercio o Comercio Secundario debe haber comprobado que la actividad del Comercio o Comercio Secundario acata completamente las leyes correspondientes a MasterCard, al Comercio o Comercio Secundario, al Emisor, al Adquiriente y a cualquier posible cliente del Comercio o Comercio Secundario. Dicha verificación puede incluir, entre otras, una opinión por escrito de un asesor legal calificado, independiente y de buena reputación o la acreditación de un tercero reconocido.

Al inscribir a un Comercio o Comercio Secundario según se requiere en esta sección, el Adquiriente representa y garantiza que ha verificado el acatamiento de las leyes correspondientes según se describe arriba. El Adquiriente debe conservar una copia de dicha verificación mientras adquiera Transacciones del Comercio o Comercio Secundario que está sujeto al requisito de inscripción descrito anteriormente y debe confirmar, con una frecuencia no menor a cada 12 meses, el acatamiento permanente de las leyes correspondientes con relación al negocio del Comercio o Comercio Secundario inscrito. El Adquiriente debe proporcionar a MasterCard una copia de dicha documentación de manera oportuna a solicitud.

9.4.4—Comercios de Lotería propiedad del Gobierno

Los siguientes requisitos aplican a los Comercios de lotería estatal en la Región de EE. UU. (consulte la sección 9.4.4.1) y a los Comercios de lotería gubernamental en Brasil y en la Región de Canadá (consulte la sección 9.4.4.2) respectivamente.

9.4.4.1 State Lottery Merchants (U.S. Region Only)

A U.S. Region Acquirer must:

- use MCC 7800 (Government Owned Lottery) to identify Transactions arising from a U.S. Region Merchant or Submerchant and involving the purchase of a state lottery ticket; and
- register each such Merchant or Submerchant with MasterCard as described in section 9.2 and this section 9.4.4.1.

To register a Merchant or Submerchant, the Acquirer must demonstrate that an adequate due diligence review was conducted by providing the following items to MasterCard as part of the registration process (herein, all references to a Merchant also apply to a Submerchant):

1. **Evidence of legal authority.** The Acquirer must provide:
   - a copy of the Merchant's license (or similar document), if any, issued by the appropriate governmental (for example, state or tribal) authority, that expressly authorizes the Merchant to engage in the gambling activity; and
   - any law applicable to the Merchant that permits state lottery ticket sales.
2. **Legal opinion.** The Acquirer must obtain a reasoned legal opinion, addressed to the Acquirer, from a private sector U.S. lawyer or U.S. law firm. The legal opinion must:
   - identify all relevant state lottery and other laws applicable to the Merchant;
   - identify all relevant state lottery and other laws applicable to Cardholders permitted by the Merchant to transact with the Merchant; and
   - demonstrate that the Merchant's and Cardholders' state lottery and payment activities comply at all times with any laws identified above.

   The Acquirer must provide MasterCard with a copy of such legal opinion. The legal opinion must be acceptable to MasterCard in its sole discretion.
3. **Effective controls.** The Acquirer must provide certification from a qualified independent third party demonstrating that the Merchant's systems for operating its state lottery business:
   - include effective age and location verification; and
   - are reasonably designed to ensure that the Merchant's state lottery business will remain within legal limits (including in connection with interstate Transactions).

   The certification must include all screenshots relevant to the certification (for example, age verification process). Certifications from interested parties (such as the Acquirer, ISOs, the Merchant, and so on) are not acceptable substitutes for the independent third-party certification.
4. **Notification of changes.** The Acquirer must certify that it will notify MasterCard of any changes to the information that it has provided to MasterCard, including changes in

applicable law, Merchant activities, and Merchant systems. Such notification shall include any revisions or additions to the information provided to MasterCard (for example, legal opinion, third-party certification) to make the information current and complete. Such notification is required within ten (10) days of any such change.

5. **Acceptance of responsibilities.** The Acquirer must specifically affirm that it will not submit restricted Transactions from the Merchant for authorization. The Acquirer must also specifically reaffirm its indemnification to MasterCard in connection with the Acquirer's or Merchant's activities. Such reaffirmation shall specifically indicate that the Acquirer acknowledges and agrees that the Transactions constitute the Acquirer's Activity and are subject to Rule 2.3 of the *MasterCard Rules* manual, regardless of the Acquirer's compliance with MasterCard rules, policies, and procedures or these requirements.

9.4.4.2 Government-owned Lottery Merchants (Specific Countries)

A Customer located in Brazil or the Canada Region must use MCC 9406 (Government Owned Lottery Merchant [Specific Countries]) to properly identify any Merchant or Submerchant engaged in the sale of lottery tickets, recurring lottery subscriptions, or both.

Subject to applicable law and regulation, a government-administered lottery scheme may sell lottery tickets or lottery subscription services via the Internet. As set forth in section 9.2 above, an Acquirer must register any Merchant or Submerchant conducting such sale in a non-face-to-face environment.

For the avoidance of doubt, this registration requirement extends to any agent duly licensed by the appropriate government authority to sell lottery tickets online.

9.4.5 Comercios de Juegos de Habilidades (Región de EE. UU. Solamente)

Un Adquiriente de la región de EE. UU. puede usar el MCC 7994 (Galerías/Establecimientos de Juegos de Video) para identificar las Transacciones que surjan de un Comercio o Comercio Secundario de la región de EE. UU. que efectúa determinados juegos (en el presente documento, "juegos de habilidades") si el Adquiriente ha inscrito primero al Comercio o Comercio Secundario en MasterCard según se describe en la sección 9.2 y esta sección 9.4.6. A los efectos de esta sección, "juegos de habilidades" significa:

- los participantes del juego pagan un cargo de ingreso al juego;
- el resultado del juego está determinado por la habilidad de los participantes en lugar de por el azar;
- el ganador de un juego recibe dinero en efectivo y/o un premio de valor monetario; y
- ninguna persona que no participe en el juego recibe dinero en efectivo y/o un premio de valor monetario relacionado con el juego.

Para inscribir a un Comercio o Comercio Secundario, el Adquiriente debe demostrar que se efectuó una revisión de diligencia debida adecuada, proporcionando los siguientes elementos a MasterCard como parte del proceso de inscripción (en el presente documento, todas las referencias a un Comercio también aplican a un Comercio Secundario):

1. **Evidencia de la autoridad legal.** El Adquiriente debe proporcionar:

- una copia de la licencia del Comercio (o documento similar), si existe, emitida por la autoridad gubernamental adecuada (por ejemplo el estado o tribu), que autorice claramente al Comercio a efectuar el tipo particular de juego de habilidades para el cual desea aceptar Tarjetas como forma de pago para los cargos de ingreso; y
- cualquier ley aplicable al Comercio que permita que se efectúen los juegos de habilidades.

2. **Opinión legal.**El Adquiriente debe obtener una opinión legal justificada, dirigida al Adquiriente, de un abogado de EE. UU. o firma legal de EE. UU. del sector privado. La opinión legal debe:

   - identificar todas las leyes relevantes relacionadas con la realización de juegos de habilidades (por ej.: leyes contra juegos de azar que incluyen una excepción para los juegos de habilidades) y otras leyes aplicables a las actividades de juegos de habilidades del Comercio;
   - identificar todas las leyes pertinentes relacionadas con la participación en los juegos de habilidades y otras leyes aplicables a los Tarjetahabientes a quienes el Comercio permite participar en los juegos de habilidades con el Comercio; y
   - demostrar que los juegos de habilidades y las actividades de pago del Comercio y del Tarjetahabiente cumplen en todo momento con las leyes identificadas anteriormente.

   El Adquiriente debe proporcionar a MasterCard una copia de dicha opinión legal. La opinión legal debe ser aceptable para MasterCard a su entera discreción.
3. **Controles eficaces.**El Adquiriente debe proporcionar la certificación de un tercero independiente calificado que demuestre que los sistemas del Comercio para las operaciones de su negocio de juegos de habilidades:

   - incluyen la verificación eficaz de la edad y la ubicación, según corresponda; y
   - están diseñados razonablemente para asegurar que el negocio de juegos de habilidades del Comercio permanecerá dentro de los límites legales (incluyendo las leyes relacionadas con Transacciones interestatales).

   La certificación debe incluir todas las capturas de pantalla pertinentes a la certificación (por ejemplo, el proceso de verificación de la edad). Las certificaciones de las partes interesadas (como el Adquiriente, la ISO, el Comercio, etcétera) no son sustitutos aceptables de la certificación de un tercero independiente.
4. **Notificación de cambios.**El Adquiriente debe certificar que notificará a MasterCard cualquier cambio a la información que ha proporcionado a MasterCard, incluyendo los cambios a las leyes aplicables, las actividades del Comercio y los sistemas del Comercio. Dicha notificación debe incluir cualquier revisión o adición a la información proporcionada a MasterCard (por ejemplo, la opinión legal, la certificación de terceros) para actualizar y completar la información. Dicha notificación se debe proporcionar dentro de los primeros diez (10) días a partir de que se efectuó el cambio.
5. **Aceptación de las responsabilidades.** El Adquiriente debe afirmar específicamente que no presentará Transacciones Restringidas (según se define en la *Política de Juegos de Azar por Internet*) del Comercio para la autorización. El Adquiriente también debe reafirmar específicamente su indemnización a MasterCard en conexión con las actividades del Adquiriente o del Comercio. Dicha reafirmación debe indicar específicamente que el Adquiriente reconoce y acuerda que las Transacciones constituyen la Actividad del

Adquiriente y que están sujetas a la Regla 3.3 de MasterCard independientemente del acatamiento del Adquiriente con las reglas, políticas y procedimientos de MasterCard o con estos requisitos.

9.4.6 Comercios de Cyberlocker de Alto Riesgo

Una Transacción de cyberlocker de alto riesgo que no es cara a cara ocurre en un entorno sin Tarjeta presente cuando un consumidor usa una cuenta para comprar el acceso directamente de un Comercio o Comercio Secundario, o indirectamente de un operador o de una entidad que puede proporcionar el acceso, a los servicios de compartir y almacenar archivos digitales a distancia.

Antes de que un Adquiriente pueda procesar Transacciones de cyberlocker de alto riesgo que no son cara a cara de un Comercio o Comercio Secundario, debe inscribir al Comercio o Comercio Secundario, y a cualquier entidad que pueda proporcionar acceso al contenido o a los servicios de dicho Comercio o Comercio Secundario, con MasterCard según se describe en la sección 9.2 de este manual.

Además, antes de que un Adquiriente pueda procesar Transacciones de cyberlocker de alto riesgo que no son cara a cara de una entidad que puede proporcionar acceso o aceptar pagos en nombre del contenido y los servicios de un Comercio o Comercio Secundario de cyberlocker, debe inscribir a la entidad y a los Comercios de cyberlocker para los cuales proporciona el acceso, con MasterCard según se describe en la sección 9.2 de este manual.

Cualquier Comercio, Comercio Secundario o entidad de cyberlocker que proporciona acceso o acepta pagos en nombre del contenido o de los servicios de dicho Comercio o Comercio Secundario de cyberlocker que cumple con uno o más de los siguientes criterios, debe ser inscrito por el Adquiriente como un Comercio de cyberlocker de alto riesgo y MasterCard determinará, a su exclusiva discreción, si el Comercio, Comercio Secundario o la entidad es un Comercio de cyberlocker de alto riesgo:

- El Comercio de cyberlocker proporciona recompensas, pagos en efectivo u otros incentivos a los usuarios que cargan datos. Algunos incentivos se basan en la cantidad de veces que se descargan los archivos del usuario o que son trasmitidos por un tercero. Los programas de recompensas del Comercio también pagan una comisión mayor por la distribución de archivos de tamaño consistente con el contenido extenso sujeto a los derechos de autor tal como películas y programas de televisión.
- El Comercio de cyberlocker proporciona códigos del URL a los usuarios que cargan datos para que sea más fácil compartir e incorporar dichos enlaces en los sitios web de índices de terceros o con enlaces.
- Los enlaces al contenido prohibido almacenados en el cyberlocker se encuentran, a menudo, en los sitios de índice de terceros o con enlaces, o por medio de consultas de los motores de búsqueda.
- Si no se obtiene acceso a los archivos almacenados dentro del Comercio de cyberlocker, se pueden depurar, a menos que el usuario compre una membresía premium.
- Los incentivos para las membresías premium de cyberlocker se basan en una mayor velocidad de descarga o en la eliminación de avisos publicitarios, en lugar del espacio de almacenamiento. De otra manera, el acceso gratuito a los archivos almacenados puede ser

desalentador debido a largos tiempos de espera, reducción del ancho de banda, límites de descarga, publicidad en línea y otras técnicas.

- El Comercio de cyberlocker proporciona un "verificador de enlaces" que permite a los usuarios determinar si se ha eliminado un enlace y, en ese caso, permite al usuario volver a cargar ese contenido rápidamente.
- Los propietarios del archivo:
  - Por lo general son anónimos,
  - No tienen que proporcionar información de identificación, y
  - No conocen la identidad de los usuarios que tienen acceso o ven sus archivos.
- En el sitio de cyberlocker se enfatiza el servicio de distribuir y compartir archivos.
- En el sitio de cyberlocker se promueve el almacenamiento o la transferencia de tipos específicos de archivos sujetos a derechos de autor tales como películas, videos o música.
- Sin la compra de una membresía premium, la reproducción de videos incluye la visualización frecuente de avisos publicitarios.

Un Adquiriente debe identificar todas las Transacciones de cyberlocker de alto riesgo que no son cara a cara usando el MCC 4816 (Red de Computadoras/Servicios de Información) y el TCC T.

En el momento de inscribir a un Comercio, Comercio Secundario o entidad conforme a esta sección, el Adquiriente de dicho Comercio, Comercio Secundario o entidad debe haber verificado que la actividad del Comercio, Comercio Secundario o entidad acata en su totalidad las leyes correspondientes a MasterCard, al Comercio, Comercio Secundario, entidad, al Emisor, Adquiriente y a cualquier posible cliente del Comercio, Comercio Secundario o entidad. Dicha verificación puede incluir, entre otras, una opinión por escrito de un asesor legal calificado, independiente y de buena reputación o la acreditación de un tercero reconocido.

Al inscribir a un Comercio, Comercio Secundario o entidad según se requiere en esta sección, el Adquiriente representa y garantiza que ha verificado el acatamiento de las leyes correspondientes según se describen arriba. El adquiriente debe conservar una copia de dicha verificación mientras adquiera Transacciones del Comercio, Comercio Secundario o entidad que está sujeto al requisito de inscripción descrito anteriormente y debe confirmar, con una frecuencia no menor a cada 12 meses, el acatamiento permanente de las leyes aplicables con relación al negocio del Comercio, Comercio Secundario o entidad inscrito. El Adquiriente debe proporcionar a MasterCard una copia de dicha documentación de manera oportuna a solicitud.

Capítulo 10 Normas y Programas de la Protección de los Datos de la Cuenta

Este capítulo puede ser de especial interés para el personal del cliente responsable de proteger los datos de la Cuenta, del Tarjetahabiente y de la Transacción; y para los Clientes que han experimentado o desean protegerse de los eventos de compromiso de datos de la cuenta.

10.1 Normas de la Protección de los Datos de la Cuenta

Las Normas de Seguridad de la PCI son requisitos técnicos y operativos establecidos por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (SSC de la PCI) como punto de referencia mínimo para proteger los datos de la Cuenta. MasterCard requiere que todos los Clientes que almacenan, procesan o transmiten datos de Tarjetas, de Tarjetahabientes o de Transacción y todos los agentes del Cliente que almacenan, procesan o transmiten datos de Tarjetas, de Tarjetahabientes o de Transacción en nombre del Cliente acaten el Programa de Seguridad de Transacción del PIN de la Industria de Tarjetas de Pago (PTS de la PCI) y la *Norma de Seguridad de Datos de la Industria de Tarjetas de Pago* (DSS de la PCI) más actuales. Las Normas de Seguridad de la PCI están disponibles en el sitio web SSC de la PCI en http://www_es-la.pcisecuritystandards.org.

10.2 Eventos de Compromiso de los Datos de la Cuenta

NOTA: Esta sección 10.2 aplica a las Transacciones de MasterCard y Maestro, salvo que se indique lo contrario.

Definiciones

Según se usan en esta sección 10.2, los siguientes términos tendrán el significado establecido a continuación:

Evento de Compromisos de los Datos de Cuenta o Evento de ADC

Un incidente que da como resultado, de manera directa o indirecta, el acceso no autorizado a datos de la Cuenta o la divulgación de los mismos o la manipulación no autorizada de controles de los datos de la Cuenta, tales como el uso de la Cuenta y los límites de gastos.

Agente

Cualquier entidad que almacena, procesa o tiene acceso a datos de la Cuenta en virtud de su relación contractual o de otra relación, directa o indirecta, con un Cliente. Para evitar dudas, los Agentes incluye, entre otros, a Comercios, Procesadores Terceros (TPP) y Entidades de Almacenamiento de Datos (DSE) (independientemente de si los TPP o DSE están inscritos con MasterCard).

Cliente

Este término aparece en el apéndice Definiciones al final de este manual. Con el fin de evitar dudas, para propósitos de esta sección 10.2, toda entidad que MasterCard habilite a emitir Tarjetas de MasterCard y/o Maestro y/o a adquirir Transacciones de MasterCard y/o Maestro será considerada como un Cliente.

Cliente de Actividad Digital

Este término aparece en el apéndice Definiciones al final de este manual. Con el fin de evitar dudas, a los efectos de esta sección 10.2, toda entidad que MasterCard haya

aprobado para ser un Solicitante de Token de Billetera será considerada como un Cliente de Actividad Digital. Un Cliente de Actividad Digital es un tipo de Cliente.

Terminal de POS Híbrida

Una terminal que (i) es capaz de procesar Transacciones con chip y Transacciones de banda magnética; y (ii) tiene el hardware, software, y la configuración equivalentes a una Terminal con estado de aprobación total de tipo de Nivel 1 y Nivel 2 de EMV con respecto a las especificaciones técnicas del chip; y (iii) ha completado satisfactoriamente el Proceso de Integración de la Terminal (TIP) de MasterCard en el entorno de uso apropiado.

Evento Potencial de Compromisos de los Datos de Cuenta o Evento Potencial de ADC

Un incidente que puede dar como resultado, de manera directa o indirecta, el acceso no autorizado a datos de la Cuenta o la divulgación de los mismos o la manipulación no autorizada de controles de los datos de la Cuenta, tales como el uso de la Cuenta y los límites de gastos.

Datos Sensibles de Autenticación de la Tarjeta.

Este término tiene el significado establecido en la *Norma de Seguridad de Datos de la Industria de Tarjetas de Pago*, e incluye, entre otras cosas, el total de los contenidos de la banda magnética de una Tarjeta o el equivalente en un chip, los datos del código de validación de la Tarjeta 2 (CVC 2) y los datos del PIN o de bloqueo del PIN.

Normas

Este término aparece en el apéndice Definiciones al final de este manual.

Solicitante de Token de Billetera

Este término aparece en el apéndice Definiciones al final de este manual.

Los términos que se usan en esta sección 10.2 (tales como Emisor, Adquiriente y Tarjeta) se usan de manera consistente con las definiciones de dichos términos en el apéndice de definiciones al final de este manual. Con respecto a las cuentas y la emisión de tarjetas, las normas de MasterCard reflejan el uso de diferentes tipos de estructuras y relaciones de licencias, que incluyen:

- Cliente principal y Cliente afiliado;
- Cliente asociado y Cliente afiliado;
- Licenciatario Principal de Débito y Licenciatario Afiliado de Débito; y
- TPP Tipo I y Cliente Afiliado (de la región de EE. UU. solamente).

A los fines de la presente Sección 10.2, un emisor será la entidad responsable de acuerdo a las normas, y si aplica, a contratos de licencia entre la entidad y MasterCard respecto a la actividad en alguna tarjeta o cuenta en particular.

10.2.1 Política Sobre los Eventos de Compromiso de los Datos de la Cuenta y Eventos Potenciales de Compromiso de los Datos de la Cuenta

MasterCard opera un sistema de soluciones de pago para todos sus Clientes. Todos los Clientes se benefician y dependen de la integridad de ese sistema. Los Eventos de ADC y los Eventos Potenciales de ADC amenazan la integridad del sistema de MasterCard y socavan la confianza de los Comercios, Clientes, Tarjetahabientes y del público en general en la seguridad y viabilidad del sistema. Cada Cliente, por lo tanto, reconoce que MasterCard tiene un interés

real en adoptar, interpretar y hacer cumplir sus Normas para proteger frente a Eventos de ADC y Eventos Potenciales de ADC y responder a los mismos.

Dada la abundancia y la sofisticación de los delincuentes, los Eventos de ADC y los Eventos Potenciales de ADC son riesgos inherentes a la operación y a la participación en cualquier sistema que utiliza los datos de las cuentas de tarjetas de pago para las transacciones financieras o no financieras. Las Normas de MasterCard están diseñadas para atribuir la responsabilidad por los eventos de ADC y de los Eventos Potenciales de ADC al Cliente que está en la mejor posición de proteger contra el riesgo y de responder ante dicho riesgo. Ese Cliente generalmente es el Cliente cuya red, sistema, o entorno resultó comprometido o fue vulnerable a la intrusión o que tiene una relación directa o indirecta con un Agente cuya red, sistema, o entorno resultó comprometido o fue vulnerable a la intrusión. En la opinión de MasterCard, ese Cliente está en la mejor posición de salvaguardar sus sistemas, exigir y vigilar la protección de los sistemas de sus Agentes y de asegurarse frente a Eventos de ADC y Eventos Potenciales de ADC y responder a los mismos.

MasterCard requiere que cada Cliente aplique la mayor diligencia y contundencia para ofrecer protección frente a Eventos de ADC y Eventos Potenciales de ADC y responder a los mismos. Cada Cliente reconoce y acepta que MasterCard tiene el derecho y la necesidad de obtener la información completa (según lo determine MasterCard) sobre las causas y efectos de un Evento de ADC o de un Evento Potencial de ADC así como también la autoridad para imponer recargos, recuperar costos y administrar la compensación, si correspondiera, a los Clientes que han incurrido en costos, gastos, pérdidas y/u otras responsabilidades en relación con los Eventos de ADC y los Eventos Potenciales de ADC.

Excepto que expresamente se estipule de otro modo en las Normas, las determinaciones de MasterCard con respecto a que han ocurrido Eventos de ADC o Eventos Potenciales de ADC y la responsabilidad por éstos, son concluyentes y no están sujetas a apelación o revisión dentro de MasterCard.

Cualquier Cliente que no esté seguro respecto a los derechos y obligaciones relacionados o que surjan en conexión a las Normas y Programas de la Protección de los Datos de la Cuenta establecidas en este Capítulo 10 debe solicitar el asesoramiento del grupo de Investigaciones de Fraude de MasterCard.

Sin perjuicio de lo anterior, la relación de las configuraciones de red, sistema y entorno con otras redes, sistemas y entornos variará a menudo, y cada Evento de ADC y Evento Potencial de ADC tiende a tener su propio conjunto de circunstancias especiales. MasterCard tiene el derecho exclusivo a interpretar y hacer cumplir las Normas, incluyendo las que están estipuladas en este capítulo. Conforme a lo precedente y de acuerdo a las definiciones estipuladas en la sección 10.2 anterior, MasterCard puede determinar, a título preliminar, si unas circunstancias dadas constituyen un Evento de ADC o varios Eventos de ADC. A este respecto, y a modo de ejemplo, cuando un Cliente o Comercio se conecta, utiliza, accede o participa en una red, sistema o entorno común con uno o más Clientes, Comercios, Proveedores de Servicios o terceros, una trasgresión de la red, sistema o entorno común que resulte, directa o indirectamente, en el compromiso de las redes, sistemas o entornos locales relacionados, puede considerarse que constituye un solo Evento de ADC.

10.2.2 Responsibilities in Connection with ADC Events and Potential ADC Events

The Customer whose system or environment, or whose Agent's system or environment, was compromised or vulnerable to compromise (at the time that the ADC Event or Potential ADC Event occurred) is fully responsible for resolving all outstanding issues and liabilities to the satisfaction of MasterCard, notwithstanding any subsequent change in the Customer's relationship with any such Agent after the ADC Event or Potential ADC Event occurred. In the event of any dispute, MasterCard will determine the responsible Customer(s).

Should a Customer, in the judgment of MasterCard, fail to fully cooperate with the MasterCard investigation of an ADC Event or Potential ADC Event, MasterCard (i) may infer that information sought by MasterCard, but not obtained as a result of the failure to cooperate, would be unfavorable to that Customer and (ii) may act upon that adverse inference in the application of the Standards. By way of example and not limitation, a failure to cooperate can result from a failure to provide requested information; a failure to cooperate with MasterCard investigation guidelines, procedures, practices, and the like; or a failure to ensure that MasterCard has reasonably unfettered access to the forensic examiner.

A Customer may not, by refusing to cooperate with the MasterCard investigation, avoid a determination that there was an ADC Event. Should a Customer fail without good cause to comply with its obligations under this section 10.2 or to respond fully and in a timely fashion to a request for information to which MasterCard is entitled under this section 10.2, MasterCard may draw an adverse inference that information to which MasterCard is entitled, but that was not timely obtained as a result of the Customer's noncompliance, would have supported or, where appropriate, confirmed a determination that there was an ADC Event.

Before drawing such an adverse inference, MasterCard will notify the Customer of its noncompliance and give the Customer an opportunity to show good cause, if any, for its noncompliance. The drawing of an adverse inference is not exclusive of other remedies that may be invoked for a Customer's noncompliance.

The following provisions set forth requirements and procedures to which each Customer and its Agent(s) must adhere upon becoming aware of an ADC Event or Potential ADC Event.

10.2.2.1 Procedimientos con Plazos Precisos para los Eventos de ADC y los Eventos Potenciales de ADC

Se considera que un Cliente tiene conocimiento de un Evento de ADC o de un Evento Potencial de ADC cuando el Cliente o el Agente del Cliente por primera vez supo o, en el ejercicio de prácticas de seguridad razonables, debió haber sabido de un Evento de ADC o un Evento Potencial de ADC. Se considera que un Cliente o su Agente tiene conocimiento de un Evento de ADC o de un Evento Potencial de ADC en las circunstancias que incluyen, entre otras, cualquiera de las siguientes:

- el Cliente o su Agente es informado, mediante cualquier fuente, de la instalación o existencia de cualquier código malicioso en cualquiera de sus sistemas o entornos, o cualquier sistema o entorno de uno de sus agentes, sin importar donde dicho código malicioso se localice o de qué modo fue introducido;

- el Cliente o su Agente reciben notificación de MasterCard o de cualquier otra fuente que el Cliente o su(s) Agente(s) ha(n) experimentado un Evento de ADC o un Evento Potencial de ADC; o
- el Cliente o su Agente descubren o, en el ejercicio de una diligencia razonable, deberían haber descubierto una violación a la seguridad o una penetración no autorizada de sus propios sistemas o entornos, o en el sistema o entorno de su(s) Agente(s).

Un Cliente debe notificar a MasterCard inmediatamente cuando el Cliente toma conocimiento de un Evento de ADC o de un Evento Potencial de ADC en o afectando cualquier sistema o entorno del Cliente o su Agente. Además, un Cliente debe, por contrato, asegurar que su Agente notifica a MasterCard inmediatamente cuando toma conocimiento de un Evento de ADC o de un Evento Potencial de ADC en o afectando cualquier sistema o entorno del Cliente o su Agente.

Cuando un Cliente o su Agente toma conocimiento de un Evento de ADC o de un Evento Potencial de ADC, en cualquier de sus propios sistemas o entornos o en los sistemas o entornos de sus Agentes, el Cliente debe tomar (o solicitar que el Agente tome) las siguientes medidas, a menos que MasterCard indique lo contrario por escrito.

- Iniciar inmediatamente una investigación detallada del Evento de ADC o del Evento Potencial de ADC.
- Inmediatamente, y a más tardar dentro de veinticuatro (24) horas, identificar, contener y mitigar el Evento de ADC o el Evento Potencial de ADC, asegurar los datos de la Cuenta y preservar toda la información, en todos los medios, relacionada con el Evento de ADC o con el Evento Potencial de ADC, incluyendo:

    1. preservar y proteger toda la evidencia potencial pertinente a un examen forense de un Evento de ADC o de un Evento Potencial de ADC;
    2. aislar los sistemas y los medios comprometidos de la red;
    3. preservar todos los Sistemas de Detección de Intrusión, los registros del Sistema de Prevención de Intrusión, todos los registros de barrera de protección, Web, base de datos y eventos;
    4. documentar todas las acciones de respuesta al incidente; y
    5. abstenerse de reiniciar o reinicializar cualquier sistema comprometido o potencialmente comprometido o tomar una acción equivalente u otra acción que tenga el efecto de eliminar o destruir información que pudiera potencialmente proporcionar evidencia acerca de un Evento de ADC o de un Evento Potencial de ADC.
- Dentro de veinticuatro (24) horas, y continuamente de allí en adelante, presentar a MasterCard todos los hechos conocidos o sospechados relacionados con el Evento de ADC o con el Evento Potencial de ADC, incluyendo, como ejemplo y sin límite, los hechos conocidos o sospechados de la causa u origen del Evento de ADC o del Evento Potencial de ADC.
- Dentro de veinticuatro (24) horas y durante toda la investigación y a partir de entonces, proporcionar a MasterCard, en el formato requerido, todos los PAN asociados con los datos de la Cuenta que fueron de hecho o potencialmente accedidos o divulgados en relación con el Evento de ADC o de un Evento Potencial de ADC, y cualquier información adicional solicitada por MasterCard. Según se usa aquí, la obligación de obtener y proporcionar los PAN para MasterCard aplica a cualquier número de cuenta de MasterCard o Maestro en un

rango de número de identificación bancaria (BIN)/número de identificación del Emisor (IIN) asignado por MasterCard. Esta obligación aplica independientemente de cómo o por qué dichos PAN fueron recibidos, procesados o almacenados, incluyendo, a modo de ejemplo y entre otros, en conexión con o relacionado a un propietario de crédito, débito (basado en la firma o en el PIN) o cualquier otro tipo de Transacción de pago, incentivo o programa de recompensas.

- Dentro de setenta y dos (72) horas, contratar los servicios de un Investigador Forense (PFI) de la SSC de la PCI para que realice una investigación forense independiente para evaluar la causa, el alcance, la magnitud, la duración y los efectos del Evento de ADC o del Evento Potencial de ADC. El PFI contratado para realizar la investigación no debe haber proporcionado el último informe de acatamiento con la PCI relacionado con el sistema o entorno que se va a examinar. Antes de que comience la investigación de dicho PFI, el Cliente debe notificar a MasterCard el alcance y la naturaleza propuestos de la investigación y obtener la aprobación preliminar de MasterCard de dicha propuesta o, si no se obtiene dicha aprobación preliminar, de una propuesta modificada aceptable para MasterCard. MasterCard y el Cliente o los Clientes responsables pueden acordar que la investigación del PFI, los hallazgos de la investigación y las recomendaciones del PFI que no afecten a todos los Comercios (u otros Agentes) dentro del ámbito de un Evento de ADC o de un Evento Potencial de ADC se considerarán representativos y se usarán con fines de aplicación de las Normas, de los hallazgos y las recomendaciones de la investigación del PFI con respecto a todos los Comercios (u otros Agentes) en el ámbito de un Evento de ADC o de un Evento Potencial de ADC.
- Dentro de dos (2) días hábiles a partir de la fecha en que el PFI fue contratado, identifique a MasterCard el PFI contratado y confirme que dicho PFI ha comenzado su investigación.
- Dentro de cinco (5) días hábiles a partir del inicio de una investigación forense, asegúrese de que el PFI somete a MasterCard un informe forense preliminar que detalle todos los hallazgos investigativos hasta la fecha.
- Dentro de veinte (20) días hábiles a partir del inicio de la investigación forense, proporcione a MasterCard un informe forense final detallando todos los hallazgos, conclusiones y recomendaciones del PFI, continúe tratando cualquier exposición notable, e implemente todas las recomendaciones hasta que el Evento de ADC o Evento Potencial de ADC sea resuelto a satisfacción de MasterCard. Con respecto a la investigación forense independiente y a la preparación del informe forense final, ningún Cliente puede comprometerse en o suscribir una (o permitir que un Agente se comprometa con o suscriba una) conducta, un convenio o entendimiento que pueda afectar la integridad, precisión u objetividad de cualquier aspecto de la investigación forense o el informe forense final. El Cliente no debe comprometerse en ninguna conducta (o permitir que un Agente se comprometa en ninguna conducta) que pudiera o fuera a influenciar o socavar la independencia de, el PFI o socavar la confiabilidad o integridad de la investigación forense o el informe forense final. A modo de ejemplo, y sin carácter limitativo, un Cliente no debe él mismo, o permitir que ninguno de sus Agentes, tome cualquier acción o deje de tomar acción que pudiera tener el efecto de:

  1. impedir, prohibir o inhibir al PFI comunicarse directamente con MasterCard;
  2. permitir que un Cliente o su Agente edite sustancialmente o por demás altere el informe forense; o

3. o indicarle al PFI que oculte información a MasterCard.

No obstante lo anterior, MasterCard puede contratar a un PFI en nombre del Cliente a fin de agilizar la investigación. El Cliente en nombre de quien se contrata el PFI será responsable de todos los costos asociados con la investigación.

10.2.2.2 Procedimientos Permanentes para los Eventos de ADC y los Eventos Potenciales de ADC

Desde el momento en que el Cliente o su Agente tienen conocimiento de un Evento de ADC o de un Evento Potencial de ADC hasta que la investigación se haya efectuado a satisfacción de MasterCard, el Cliente debe:

- Proporcionar informes por escrito semanales del estado que contengan información real, exacta y actualizada referente al Evento de ADC o al Evento Potencial de ADC, los pasos que se están adoptando para investigar y remediar los mismos y cualquier otra información que MasterCard pueda solicitar.
- Conservar todos los archivos, datos y otra información pertinente al Evento de ADC o al Evento Potencial de ADC, y abstenerse de tomar cualquier medida (por ejemplo, el reinicio) que pudiera tener como resultado la alteración o pérdida de cualquiera de estos archivos, fuentes de datos forenses, incluyendo archivos de registro de eventos y de barrera de protección, u otra información.
- Dar una respuesta de manera completa y rápida, de la forma prescrita por MasterCard, a cualquier pregunta u otra solicitud (incluyendo las solicitudes de seguimiento) de MasterCard respecto al Evento de ADC o al Evento Potencial de ADC y los pasos que se están adoptando para investigar y remediarlo.
- Autorizar y solicitar al PFI que proporcione una respuesta de manera completa, directa y rápida a cualquier pregunta escrita u verbal, o a otras solicitudes de MasterCard y, de este modo responder en la manera prescrita por MasterCard, con respecto al Evento de ADC o al Evento Potencial de ADC, que incluye los pasos que se están adoptando para investigar y remediarlo.
- Estar de acuerdo con, y cooperar con, cualquier esfuerzo de MasterCard para contratar y dirigir a un PFI para realizar una investigación y preparar un informe forense referente al Evento del ADC o al Evento Potencial de ADC, en el caso de que el Cliente no pueda satisfacer cualquiera de las responsabilidades anteriores.
- Asegurar que la entidad comprometida desarrolla un plan de acción de solución, que incluye las fechas de implementación y las fechas importantes referentes a los hallazgos, las medidas correctivas y las recomendaciones identificadas por el PFI y descritas en el informe forense final.
- Controlar y validar que la entidad comprometida ha implementado por completo el plan de acción de solución, las recomendaciones y las medidas correctivas.

10.2.3 Informe Forense

El Cliente responsable (o su Agente) debe de asegurarse de que el PFI retenga y proteja todos los informes forenses relacionados a un Evento de ADC o Evento Potencial de ADC, y a petición de MasterCard proveer inmediatamente a MasterCard cualquiera de dichos informes.

El informe forense final requerido bajo la sección 10.2.2.1 debe incluir lo siguiente, a menos que MasterCard indique lo contrario por escrito:

- Una declaración del alcance de la investigación, incluyendo fuentes de evidencia e información usada por el PFI.
- Un diagrama de la red, incluyendo todos los sistemas y componentes de red dentro del alcance de la investigación forense. Como parte de este análisis, se deben identificar todas las versiones de software y hardware del sistema, incluyendo las aplicaciones del POS y las versiones de las aplicaciones y hardware usados por la entidad comprometida dentro de los pasados doce (12) meses.
- Un flujo de Transacción de Tarjeta de pago representando todos los POI asociados con la transmisión, el procesamiento y el almacenamiento de los datos de la Cuenta y los diagramas de la red.
- Un análisis escrito explicando el o los método(s) usado(s) para violar la red o el entorno de dicha entidad así como el o los método(s) usado(s) para acceder y copiar los datos de la Cuenta.
- Un análisis por escrito explicando cómo se detuvo la violación a la seguridad y los pasos (y las fechas importantes de los pasos) que se han dado para asegurar que los datos de las Cuenta ya no se encuentran en riesgo de estar comprometidas.
- Una explicación de la metodología de investigación así como la identificación de las fuentes de los datos forenses usadas para determinar los resultados del reporte final.
- La determinación y caracterización de los datos de la Cuenta que esté en riesgo de estar comprometida, a incluir el número de las Cuentas y de componentes de datos en riesgo.
- La ubicación y el número de las Cuentas donde los datos restringidos de la Cuenta, tanto si están encriptados o no, fueron o pueden haber sido almacenados por la entidad objeto de la investigación forense. Esto incluye los datos de Cuenta restringida que fueron o pueden haber sido almacenados en un espacio del disco no asignado, medios de respaldo o archivos de salida de datos de software maligno.
- Un espacio de tiempo para Transacciones relacionadas con Cuentas determinadas como en riesgo de ser comprometidas. Si no se puede determinar la fecha/hora de la Transacción, se debe proporcionar un sello de tiempo de creación de archivo.
- La determinación de si ocurrió, y de haber ocurrido, cómo se divulgaron o tomaron erróneamente los datos de la tarjeta de pago.
- En una base de requisito por requisito, una conclusión de si, a la hora en que ocurrió el Evento de ADC o un Evento Potencial de ADC, se acataba cada requisito aplicable del SSC de la PCI. A fin de evitar toda duda, a partir de la fecha de publicación de estas Normas, las Normas de Seguridad de la PCI incluyen la DSS de la PCI, Requisitos de Seguridad del Dispositivo de Ingreso del PIN (PED de la PCI), y la *Norma de Seguridad de Datos de la Aplicación de Pago* (DSS de la PA).

MasterCard puede requerir que el Cliente haga que un PFI lleve a cabo un análisis de brecha PCI e incluya el resultado de ese análisis en el informe forense final.

El Cliente debe indicarle al PFI presentar una copia del informe forense preliminar y final a MasterCard a través de Secure Upload.

10.2.4 Normas Alternativas Aplicables a Determinados Comercios u otros Agentes

En caso de un Evento de ADC o un Evento Potencial de ADC (a los efectos de esta sección 10.2.4, un "Evento") en el cual el objeto es un Comercio de Nivel 2, Nivel 3 o Nivel 4 (según se establece en la sección 10.3.4), en lugar de acatar las obligaciones del Cliente responsable establecidas en la sección 10.2.2.1, en el primer punto de la sección 10.2.2.2 y de la sección 10.2.3 de este Capítulo 10, el Cliente responsable podrá acatar las Normas establecidas en esta sección 10.2.4 siempre que se cumplan todos estos criterios:

Criterio A

MasterCard determina que menos de 30.000 Cuentas están en riesgo de divulgación no autorizada como resultado del Evento; y

Criterio B

MasterCard determina que el Comercio (u otro agente) no ha sido el objeto de un Evento de ADC o un Evento Potencial de ADC durante los treinta y seis (36) meses consecutivos inmediatamente anteriores a la fecha que MasterCard determine como la fecha más temprana posible del Evento; y

Criterio C

El Cliente responsable determina que el Comercio (u otro Agente) usa un sistema de aceptación por computadora que no comparte conectividad con otro Comercio (o Agente) o sistema del Comercio (o del Agente) y que no está operado por un Proveedor de Servicios.

Si MasterCard determina que el objeto del Evento es un Comercio de Nivel 2, 3 ó 4 y que se cumplen los Criterios A y B mencionados anteriormente, MasterCard proporcionará un aviso al Cliente responsable por medio de un mensaje de correo electrónico dirigido al Contacto de Seguridad del Cliente responsable listado en la aplicación Información del Miembro—MasterCard, disponible en MasterCard Connect™.

Después de recibir dicho aviso, el Cliente responsable puede optar por que un PFI lleve a cabo un examen del Comercio u otro agente de acuerdo con la sección 10.2.2.1 de este Capítulo 10. Si el cliente responsable opta por que un PFI lleve a cabo un examen, el cliente responsable debe de notificar a MasterCard dentro de un plazo de 24 horas de involucrar al PFI. No notificar a MasterCard dentro del plazo de 24 horas puede acarrear recargos por no acatamiento según se describe en la sección 10.2.6. Como alternativa, y siempre que el cliente responsable determine que se cumple el Criterio C, el Cliente responsable puede elegir investigar por sí mismo el Evento en lugar de que sea un PFI quien conduzca un examen del Comercio u otro agente.

Si el Cliente responsable elige conducir la investigación por sí mismo, en un plazo inferior a los treinta (30) días posteriores a la fecha del aviso por parte de MasterCard mencionado anteriormente, el Cliente responsable debe proporcionar una certificación por escrito a MasterCard por medio de un funcionario del Cliente responsable que certifique que todo lo siguiente es verdadero:

- Que el Cliente responsable eligió investigar el Evento de ADC o el Evento Potencial de ADC en lugar de solicitar que un PFI investigara el Evento de ADC o el Evento Potencial de ADC; y
- Que el Comercio (u otro Agente)que sea el sujeto del Evento de ADC o del Evento Potencial de ADC no usa un sistema de aceptación por computadora que use otro Comercio (o Agente)o Comercios (o Agentes); y
- Que la investigación del Cliente responsable del Evento de ADC o del Evento Potencial de ADC se ha completado el Evento de ADC o el Evento Potencial de ADC; y
- Que el Comercio ha validado recientemente o ha vuelto a validar el acatamiento a la DSS de la PCI. Se deberá proporcionar a MasterCard documentación que confirme dicha validación o revalidación con la certificación del agente.

Con excepción de lo estipulado específicamente en esta sección 10.2.4, todos los demás derechos y obligaciones de MasterCard y del Cliente respecto a un Evento de ADC o Evento Potencial de ADC continuarán respecto a cualquier Evento de ADC o Evento Potencial de ADC que el Cliente responsable elija investigar de acuerdo con esta sección 10.2.4. Además, y para que no haya lugar a dudas, MasterCard tiene derecho a exigir en cualquier momento que el Cliente responsable solicite a un PFI que conduzca un examen forense de un Comercio a pesar de las disposiciones de esta sección 10.2.4.

10.2.5 Determinación de MasterCard de un Evento de ADC o de un Evento Potencial de ADC

MasterCard evaluará la totalidad de las circunstancias conocidas, que incluyen entre otras lo siguiente, para determinar si un caso constituye o no un Evento de ADC o un Evento Potencial de ADC:

- un Cliente o su Agente tiene conocimiento o confirma la ocurrencia de un Evento de ADC o un Evento Potencial de ADC;
- todo informe del PFI; o
- toda información que MasterCard determine lo suficientemente confiable al momento de la recepción.

10.2.5.1 Recargos por Infracciones a la PCI en Relación a los Eventos de ADC

Con base en la totalidad de las circunstancias conocidas en torno a un Evento de ADC o a un Evento Potencial de ADC, que incluyen el conocimiento y la intención del Cliente responsable, MasterCard (además de todo recargo proporcionado en cualquier parte de estas Normas) podrá imponer un recargo a un Cliente responsable de hasta USD 100.000 por cada violación de un requisito del SSC de la PCI.

10.2.5.2 Reducción Potencial de la Responsabilidad Financiera

A pesar de la determinación de MasterCard de que tuvo lugar un Evento de ADC, MasterCard puede considerar cualquier medida tomada por la entidad comprometida para establecer, implementar y mantener procedimientos y mejores prácticas de apoyo para salvaguardar los datos de la Cuenta antes de, durante, y después de un Evento de ADC o un Evento Potencial de ADC, con el fin de eximir, parcial o completamente, a un Cliente de otro modo responsable de la responsabilidad por cualquier recargo, reembolso operativo de ADC, costos de

investigación y/o recuperación por fraude de ADC. Al determinar si eximir a un Cliente responsable de todas o algunas responsabilidades financieras, MasterCard puede considerar si el Cliente ha acatado todos los requisitos siguientes:

- Sustentación a MasterCard de un Asesor de Seguridad Calificado (QSA) aprobado por el SSC de la PCI del acatamiento de la entidad comprometida con el DSS de la PCI en el momento del Evento de ADC o del Evento Potencial de ADC.
- Informes que certifican que todo Comercio relacionado con el Evento de ADC o el Evento Potencial de ADC acata el DSS de la PCI y todos los requisitos del Programa de Protección de los Datos del Sitio (SDP) de MasterCard en el momento del Evento de ADC o Evento Potencial de ADC de acuerdo con la sección 10.3.3 de este manual. Estos informes también deben confirmar que todas las aplicaciones de pago proporcionadas por terceros utilizadas por los Comercios asociados al Evento de ADC o Evento Potencial de ADC están en acatamiento con la *Norma de Seguridad de Datos de la Aplicación de Pago de la Industria de las Tarjetas de Pago*, según corresponda. La aplicabilidad de la DSS de la PA de la PCI a las aplicaciones de pago proporcionadas por terceros se define en la *PCI PA-DSS Program Guide* que se encuentra en pcisecuritystandards.org.
- Si la entidad comprometida es un Comercio de la Región de Europa, un PFI ha validado que el Comercio está en acatamiento con los objetivos importantes del uno al cuatro del *Enfoque de Prioridad de la DSS de la PCI* en el momento del Evento de ADC o del Evento Potencial de ADC.
- Inscripción a todo TTP o DSE asociado(s) con el Evento de ADC mediante MasterCard Connect, de acuerdo con el Capítulo 7 del *Reglamento de MasterCard*.
- Notificación de un Evento de ADC o un Evento Potencial de ADC a y cooperación con MasterCard y, según el caso, con las autoridades públicas.
- Verificación de que investigación forense se inició dentro de las setenta y dos (72) horas siguientes al Evento de ADC o al Evento Potencial de ADC y se terminó lo más pronto posible.
- Recepción oportuna por parte de MasterCard de los hallazgos de las pruebas forenses sin editar (por otra persona que no sea el examinador forense).
- Evidencia de que el Evento de ADC o Evento Potencial de ADC no era previsible o evitable por medios comerciales razonables y que, de forma constante, se aplicaron las mejores prácticas de seguridad.

En relación con su evaluación de las medidas del Cliente o su Agente, MasterCard considerará, y podrá sacar conclusiones adversas de, la evidencia de que un Cliente o su(s) Agente(s) eliminó o modificó datos.

Tan pronto como sea posible, MasterCard se comunicará con el Contacto de Seguridad del Cliente, el Contacto Principal o el Contacto de Compromiso de los Datos de la Cuenta según aparecen en la lista de la solicitud de Información del Miembro, para notificar a todas las partes afectadas de la compensación u obligación financiera inminente, según corresponda.

Es responsabilidad exclusiva de cada Cliente, no de MasterCard, incluir la información completa y actual en la aplicación de Información del Miembro.

10.2.5.3 Reembolso Operativo del ADC y Recuperación por Fraude del ADC—MasterCard Solamente

NOTA: Esta sección aplica solamente a las Transacciones de MasterCard.

El reembolso operativo (OR) del ADC permite al Emisor recuperar parcialmente los costos incurridos por emitir nuevamente las Tarjetas y por el control mejorado de las Cuentas comprometidas y/o potencialmente comprometidas de MasterCard relacionadas con un Evento de ADC. La recuperación por fraude (FR) del ADC permite al Emisor la recuperación parcial incremental de banda magnética (POS 90) y/o Terminal Híbrida de POS que no pueda procesar (POS 80) pérdidas de fraude por falsificación relacionadas con un Evento de ADC. MasterCard determina el reembolso operativo del ADC y la recuperación por fraude del ADC.

MasterCard puede invocar OR, u OR y FR (OR y FR en conjunto, el "componente de reembolso") en un Evento del ADC que impacte a 30.000 cuentas o más de MasterCard. La participación en el componente de reembolso del Programa de ADC será opcional para los emisores cada año calendario. Cada año, el emisor podrá elegir si va a participar en el componente de reembolso el siguiente año calendario. Un emisor debe escoger si va a participar en el componente de reembolso para tener derecho a recibir OR y/o FR con respecto a un Evento de ADC que MasterCard determine que ocurrió durante dicho año calendario. Para los fines de esta Sección 10.2.5.3, MasterCard en general estima que un Evento de ADC ocurrió en el año en que MasterCard publica un alerta inicial de ADC para los emisores afectados sobre un Evento de ADC. Sin embargo, MasterCard se reserva el derecho a determinar que un Evento de ADC ocurrió un año que no es el año en que MasterCard publicó la alerta inicial del ADC para los emisores afectados sobre un Evento de ADC.

Cada Emisor que escoja participar en el componente de reembolso debe aceptar, como condición para dicha participación, indemnizar y liberar de responsabilidad a MasterCard, y según sea aplicable, a cada Cliente responsable y a cada Agente de los Clientes responsables, de cualquier obligación financiera o de otro tipo directa o indirectamente relacionada a un Evento de ADC que MasterCard estime que haya ocurrido durante dicho año calendario. MasterCard le cobrará un cargo anual a principios de cada año calendario a cada emisor que decida participar en el componente de reembolso del Programa de ADC, según aplique a la región. Un emisor que decida no participar en el componente de reembolso durante un año calendario pagará un cargo anual reducido por recibir alertas de ADC, según aplique a la región.

Si MasterCard determinara que un número insuficiente de emisores ha optado participar en el componente de reembolso del Programa de ADC en un año calendario, MasterCard les notificará a los clientes de dicha decisión; en dicho caso, los emisores en cada región pagarán un cargo anual reducido por recibir alertas de ADC solamente, según aplique.

Después que concluya una investigación, se le divulgará al cliente responsable cualquier obligación relacionada al OR y/o FR en una carta definitiva de responsabilidad financiera. Los clientes responsables tendrán 30 días a partir de la fecha de la carta definitiva de responsabilidad financiera para apelar su responsabilidad. Si al concluir el proceso de apelación MasterCard determina que el cliente responsable tiene responsabilidad financiera relacionada al Evento de ADC, el cliente responsable tiene la opción de aceptar o de rechazar

el monto determinado. Como condición para aceptar el monto determinado, y respecto al Evento de ADC, el cliente responsable debe de hacer ambos de lo siguiente:

- Dentro de 14 días calendario de recibir la carta definitiva de responsabilidad financiera o la decisión de MasterCard respecto a la apelación, cualquiera de las dos que sea posterior, ejecutar y presentar a MasterCard una liberación aceptable a MasterCard en forma y sustancia que detalle que el Cliente acuerda no interponer una demanda que surja o esté relacionada con un Evento de ADC contra MasterCard o contra algún Emisor que reciba OR y/o FR; y
- Presentar a MasterCard una liberación aceptable a MasterCard en forma y sustancia ejecutada por el Comercio (u otro Agente) que detalle que el comercio (u otro Agente) acuerda no interponer una demanda que surja o esté relacionada al Evento de ADC contra MasterCard o contra algún emisor que reciba OR y/o FR.

Posteriormente, MasterCard debitará los fondos de la cuenta del cliente responsable y desembolsará OR y/o FR, según el caso, a los emisores.

Si el cliente responsable rehúsa aceptar el monto determinado, cada emisor que haya optado participar en el componente de reembolso del Programa de ADC el año en que MasterCard haya determinado que ocurrió el Evento de ADC será liberado de su renuncia a interponer demandas relacionadas al Evento de ADC contra el cliente responsable y/o el agente del cliente responsable.

Para obtener información adicional, consulte el Capítulo 6 de la *ADC User's Guide*.

En caso de que la entidad comprometida sea un comercio electrónico (e-commerce) y solo se haya comprometido el nombre del tarjetahabiente, el PAN, la fecha de vencimiento y/o la información del CVC 2, se podrá invocar solamente reembolso operativo parcial de ADC.

El reembolso operativo parcial y la recuperación por fraude parcial están disponibles para los Emisores con licencia de acceso a la aplicación Manage My Fraud & Risk Programs [Manejo de mi Fraude y Programas de Riesgo] en el momento del Evento de ADC y que hayan escogido participar en el componente de reembolso del Programa de ADC en el año calendario en que MasterCard haya estimado que ocurrió el Evento de ADC. MasterCard se reserva el derecho a determinar si algún Evento de ADC es elegible para el reembolso operativo del ADC y/o para la recuperación por fraude del ADC y de limitar o "recuperar" los reembolsos operativos del ADC y/o la recuperación por fraude del ADC según el monto cobrado al Cliente responsable, excluidos los recargos, o con el propósito de solucionar cualquier demanda alegada que surja de, o esté relacionada con, un Evento de ADC.

Con relación a un Evento de ADC en particular, MasterCard no tiene obligación de desembolsar un monto en exceso del monto que MasterCard cobra real y finalmente al Cliente responsable. En ese respecto, (i) cualquier monto cobrado real y finalmente a un Cliente responsable con relación a un Evento de ADC en particular es determinado por MasterCard de acuerdo a la resolución completa y final de cualquier reclamación alegada contra MasterCard que surja o esté relacionada con ese Evento de ADC; y (ii) cualquier fondo desembolsado por MasterCard a un Cliente como reembolso operativo del ADC y/o recuperación por fraude se desembolsa en forma condicional y sujeto a "recuperación" hasta que todas las reclamaciones alegadas contra MasterCard que surjan o estén relacionadas con el Evento de ADC se hayan resuelto total y completamente.

En la administración de los programas de ADC OR y de ADC FR, MasterCard puede determinar la responsabilidad financiera del Cliente responsable con respecto a un Evento de ADC. Cuando se determina la responsabilidad financiera, MasterCard puede tener en cuenta el nivel de la PCI de la entidad comprometida (según se establece en la sección 10.3.4), el volumen de ventas anuales y los factores establecidos en la sección 10.2.5.2.

El volumen de ventas anuales se deriva de las Transacciones de compensación del Comercio procesadas durante el año calendario anterior mediante el Sistema de Manejo de Compensación Global (GCMS). Las transacciones que no fueron procesadas por MasterCard se pueden incluir en el volumen de ventas anuales si los datos se encuentran disponibles. En el caso de que se desconozca el volumen de ventas anuales del Comercio, MasterCard utilizará el volumen de ventas existentes del Comercio para proyectar el volumen de ventas anuales o le solicitará dicho volumen al cliente responsable.

10.2.5.4 Determinación del Reembolso Operativo (OR)

NOTA: Esta sección aplica solamente a las Transacciones de MasterCard.

Sujeto a la sección 10.2.5.3, MasterCard por lo general determina el OR conforme a los siguientes pasos. MasterCard se reserva el derecho de determinar el OR de una forma alternativa si MasterCard determina que la información necesaria para seguir los siguientes pasos no está disponible de forma oportuna. Para obtener información adicional relativa al OR, consulte la *Account Data Compromise User Guide* de MasterCard.

1. MasterCard determina el número de Cuentas en riesgo por el número ICA del Emisor, por tipo de Tarjeta. Las cuentas que se hayan divulgado en una Alerta de ADC anterior en relación a un Evento de ADC diferente dentro de 180 días antes de la publicación de la Alerta de ADC por el Evento de ADC bajo investigación serán excluidas del cálculo. Vigente a partir del 31 de diciembre de 2016, las Cuentas de Tarjetas de banda magnética solamente que estén en riesgo (es decir, Cuentas de Tarjeta con Chip que no son de EMV) también serán excluidas del cálculo.
2. MasterCard multiplica el número de Cuentas en riesgo por un monto establecido por MasterCard de vez en cuando.
3. De los resultados de los Pasos 1 y 2, MasterCard podrá restar un deducible fijo (publicado en un *Boletín de Seguridad Global* o en otra publicación de MasterCard), para representar los vencimientos de la Tarjeta, y los ciclos de reemisión de Tarjetas.
4. **Región de Estados Unidos Solamente**—En la investigación de un Evento de ADC abierta por MasterCard el 1 de octubre de 2013 o posteriormente, MasterCard:

    a. Dividirá a la mitad el monto determinado en los Pasos 1, 2 y 3 mencionados, si la entidad comprometida es un Comercio de Adquiriente de la Región de EE. UU. ubicado en la Región de EE. UU. y MasterCard determina que (i) al menos el setenta y cinco por ciento (75%) del conteo total anual de Transacciones del Comercio fue procesado a través de Terminales de POS Híbridas; y (ii) al menos el setenta y cinco por ciento (75%) de las Transacciones consideradas por MasterCard como dentro del alcance del Evento de ADC, fueron procesadas a través de Terminales de POS Híbridas; y (iii) MasterCard no ha identificado al Comercio como que haya tenido un Evento de ADC diferente durante los doce (12)meses anteriores a la fecha de publicación de la

primera Alerta de ADC del Evento de ADC en cuestión; y (iv) MasterCard determina que el Comercio no almacenaba Datos Confidenciales de Autenticación de la Tarjeta; o

b. Con vigencia a partir del 1 de octubre de 2015, no cobrará una OR si la entidad comprometida es un Comercio de Adquiriente de la Región de EE. UU. ubicado en la Región de EE. UU. y MasterCard determina que (i) al menos el noventa y cinco por ciento (95%) del conteo total anual de Transacciones del Comercio fue adquirido a través de Terminales de POS Híbridas; y (ii) al menos el noventa y cinco por ciento (95%) de las Transacciones consideradas por MasterCard como dentro del alcance del Evento de ADC fueron adquiridas a través de Terminales de POS Híbridas; y (iii) MasterCard no ha identificado al Comercio como que haya tenido un Evento de ADC diferente durante los doce (12) meses anteriores a la fecha de publicación de la primera Alerta de ADC del Evento de ADC en cuestión; y (iv) MasterCard determina que el Comercio no almacenaba Datos Confidenciales de Autenticación de la Tarjeta.

   En función de este Paso 4, un conteo total anual de las Transacciones del Comercio se determina según las Transacciones de compensación del Comercio procesadas durante los doce (12) meses anteriores a la fecha de publicación de la Alerta de ADC, a través del GCMS. Las transacciones que no fueron procesadas por MasterCard se incluyen en el conteo anual de Transacciones solamente si los datos relativos a dichas transacciones están a disposición de MasterCard. En el caso de que MasterCard no pueda determinar el conteo total anual real de las Transacciones del Comercio, MasterCard podrá aplicar su criterio para determinar un conteo total anual de Transacciones. MasterCard puede solicitar que un Adquiriente le proporcione información con dicho fin.

5. **Todas las Regiones Excepto la Región de EE. UU.**—En la investigación de un Evento de ADC abierta por MasterCard el 1 de diciembre de 2014 o posteriormente, MasterCard determinará el OR de la forma establecida en el Paso 4 arriba, siempre y cuando el porcentaje requerido de las Transacciones procesadas haya sido procesado a través de Terminales de POS Híbridas.

10.2.5.5 Determinación de la Recuperación por Fraude (FR)

NOTA: Esta sección aplica solamente a las Transacciones de MasterCard.

MasterCard determina la FR de la manera que se establece en esta sección.

Sujeto a la sección 10.2.5.3, MasterCard determina un monto de fraude por falsificación incremental atribuible a un Evento de ADC basado en los datos de fraude comunicados al Sistema para Evitar el Fraude con Eficacia (SAFE). Tal como se usa en la frase inmediatamente anterior, las palabras "fraude por falsificación incremental" se refieren al fraude por falsificación incremental al fraude por falsificación que MasterCard determina se hubiera esperado que ocurriera si el Evento de ADC no hubiese ocurrido. Vigente a partir del 31 de diciembre de 2016, las Cuentas que estén en riesgo en Tarjetas de banda magnética solamente ("Cuentas de Tarjeta de banda magnética solamente") se excluirán de esta determinación y no serán elegibles para FR. Para obtener información adicional relativa a la FR, consulte *Account Data Compromise User Guide* de MasterCard.

NOTA: Si el tipo de fraude comunicado al SAFE de una o más Transacciones fraudulentas se cambia después de que MasterCard haya calculado el monto de recuperación por fraude del ADC, MasterCard no recalcula el monto de recuperación por fraude del ADC.

El cálculo de la FR usa un "período de tiempo en riesgo". El período de tiempo en riesgo puede ser conocido o desconocido.

Período de Tiempo En Riesgo Conocido

El período de tiempo en riesgo es "conocido" si MasterCard puede determinar un período de tiempo durante el cual las Cuentas estuvieron en riesgo de usarse en transacciones fraudulentas debido a o en conexión con un Evento de ADC o Evento Potencial de ADC. En ese caso, el período de tiempo en riesgo de un número de Cuenta comienza en la fecha que MasterCard determina que la Cuenta entró en riesgo, y termina en la fecha especificada en la primera Alerta de ADC relacionada con dicho Evento de ADC o Evento Potencial de ADC que divulgue ese número de Cuenta. El número de días que tiene el Emisor para informar al SAFE sobre las Transacciones fraudulentas relacionadas con un número de Cuenta divulgado en una Alerta de ADC se especifica en la alerta; un Emisor no tiene derecho a recibir FR relacionado con una Transacción fraudulenta que surja del uso de un número de Cuenta si esa Transacción fraudulenta no se informa al SAFE de forma oportuna. MasterCard determinará el número de días que el Emisor tiene para informar sobre las Transacciones fraudulentas al SAFE sobre un número de Cuenta divulgada según se indica a continuación:

- Si MasterCard publica una Alerta de ADC antes de que MasterCard haya recibido un informe definitivo del PFI con relación al Evento de ADC o al Evento Potencial de ADC, entonces dicha Alerta especificará si el Emisor tiene 30, 45 o 60 días para informar sobre las Transacciones fraudulentas al SAFE.

  NOTA: Según se establece en el Capítulo 5 de la *ADC User's Guide*, MasterCard determina el número de días en que un Emisor deberá informar al SAFE sobre las Transacciones fraudulentas con base en el número de Cuentas puestas en riesgo en el Evento de ADC o en el Evento Potencial de ADC: (i) si un Evento de ADC o Evento Potencial de ADC puso de 30.000 a 1.000.000 de Cuentas en riesgo, entonces el número de días será 30; (ii) si un Evento de ADC o Evento Potencial de ADC puso de 1.000.000 a 5.000.000 de Cuentas en riesgo, entonces el número de días será 45; o (iii) si un Evento de ADC o Evento Potencial de ADC puso al menos 5.000.000 de Cuentas en riesgo, entonces el número de días será 60.

- Si MasterCard publica una Alerta de ADC después de que MasterCard haya recibido un informe final del PFI con relación al Evento de ADC o al Evento Potencial de ADC, y MasterCard ha publicado una alerta anterior de ADC sobre un Evento de ADC, entonces dicha Alerta especificará si el Emisor tiene 20, 35 o 50 días para informar al SAFE sobre las Transacciones fraudulentas.

NOTA: Según se establece en el Capítulo 5 de la *ADC User's Guide*, MasterCard determina el número de días en que un Emisor deberá informar al SAFE sobre las Transacciones fraudulentas con base en el número de Cuentas puestas en riesgo en el Evento de ADC o en el Evento Potencial de ADC: (i) si un Evento de ADC o Evento Potencial de ADC puso de 30.000 a 1.000.000 de Cuentas en riesgo, entonces el número de días será 20; (ii) (ii) si un Evento de ADC o Evento Potencial de ADC puso de 1.000.000 a 5.000.000 de Cuentas en riesgo, entonces el número de días será 35; o (iii) si un Evento de ADC o Evento Potencial de ADC puso al menos 5.000.000 de Cuentas en riesgo, entonces el número de días será 50.

Período de Tiempo En Riesgo Desconocido

El período de tiempo en riesgo es "desconocido" si MasterCard no puede determinar fácilmente un período de tiempo en riesgo conocido. En ese caso, un período de tiempo en riesgo de un número de Cuenta comienza doce (12) meses antes de la fecha de publicación de la primera Alerta de ADC para el Evento de ADC o el evento potencial de ADC que divulgue ese número de Cuenta, y finaliza en la fecha que se especifique en dicha alerta de ADC. El número de días que tiene el Emisor para informar al SAFE sobre las Transacciones fraudulentas relacionadas con un número de Cuenta divulgado en una Alerta de ADC se especifica en la alerta; un Emisor no tiene derecho a recibir FR relacionado con una Transacción fraudulenta que surja del uso de un número de Cuenta si esa Transacción fraudulenta no se informa al SAFE de forma oportuna. MasterCard determinará el número de días que el Emisor tiene para informar sobre las Transacciones fraudulentas al SAFE sobre un número de Cuenta divulgada según se indica a continuación:

- Si MasterCard publica una Alerta de ADC antes de que MasterCard haya recibido un informe definitivo del PFI con relación al Evento de ADC o al Evento Potencial de ADC, entonces dicha Alerta especificará si el Emisor tiene 30, 45 o 60 días para informar sobre las Transacciones fraudulentas al SAFE.

  NOTA: Según se establece en el Capítulo 5 de la *ADC User's Guide*, MasterCard determina el número de días en que un Emisor deberá informar al SAFE sobre las Transacciones fraudulentas con base en el número de Cuentas puestas en riesgo en el Evento de ADC o en el Evento Potencial de ADC: (i) si un Evento de ADC o Evento Potencial de ADC puso de 30.000 a 1.000.000 de Cuentas en riesgo, entonces el número de días será 30; (ii) si un Evento de ADC o Evento Potencial de ADC puso de 1.000.000 a 5.000.000 de Cuentas en riesgo, entonces el número de días será 45; o (iii) si un Evento de ADC o Evento Potencial de ADC puso al menos 5.000.000 de Cuentas en riesgo, entonces el número de días será 60.

- Si MasterCard publica una Alerta de ADC después de que MasterCard haya recibido un informe final del PFI con relación al Evento de ADC o al Evento Potencial de ADC, y MasterCard ha publicado una alerta anterior de ADC sobre un Evento de ADC, entonces dicha Alerta especificará si el Emisor tiene 20, 35 o 50 días para informar al SAFE sobre las Transacciones fraudulentas.

NOTA: Según se establece en el Capítulo 5 de la *ADC User's Guide*, MasterCard determina el número de días en que un Emisor deberá informar al SAFE sobre las Transacciones fraudulentas con base en el número de Cuentas puestas en riesgo en el Evento de ADC o en el Evento Potencial de ADC: (i) si un Evento de ADC o Evento Potencial de ADC puso de 30.000 a 1.000.000 de Cuentas en riesgo, entonces el número de días será 20; (ii) si un Evento de ADC o Evento Potencial de ADC puso de 1.000.000 a 5.000.000 de Cuentas en riesgo, entonces el número de días será 35; o (iii) si un Evento de ADC o Evento Potencial de ADC puso al menos 5.000.000 de Cuentas en riesgo, entonces el número de días será 50.

Cuentas Divulgadas por Eventos de ADC Diferentes

Un número de Cuenta divulgado en una Alerta de ADC con relación a un Evento de ADC diferente durante los 180 días calendario anteriores a la primera divulgación de dicho número de Cuenta en una Alerta de ADC publicada con relación al Evento de ADC mencionado no es elegible para la recuperación por fraude de ADC del Evento de ADC mencionado.

Deducción en el Contracargo

Además, un deducible estándar, publicado ocasionalmente, se aplica para compensar recuperaciones de contracargos en Transacciones usando los números de Cuenta en riesgo.

Impacto del Cambio de Responsabilidad del Chip

Números de cuenta con fraude incremental por falsificación que califiquen para el contracargo del emisor bajo el código de mensaje 4870 o 70 (Cambio de Responsabilidad del Chip) no se tomarán en consideración durante el proceso de calcular la recuperación de fraude de ADC.

Para obtener información adicional con relación a los criterios usados por MasterCard al determinar el período de tiempo en riesgo, consulte el Capítulo 5 de la *ADC User's Guide*.

Solamente en la Región de Estados Unidos—MasterCard:

En una investigación de Eventos de ADC abierta por MasterCard el 1 de octubre de 2013 o posteriormente:

1. Dividirá a la mitad la FR, si la entidad comprometida es un Comercio de Adquiriente de la Región de EE. UU. ubicado en la Región de EE. UU. y MasterCard determina que (i) al menos el setenta y cinco por ciento (75%) del conteo total anual de Transacciones del Comercio fue procesado a través de Terminales de POS Híbridas; y (ii) al menos el setenta y cinco por ciento (75%) de las Transacciones consideradas por MasterCard como dentro del alcance del Evento de ADC, fueron procesadas a través de Terminales de POS Híbridas; y (iii) MasterCard no ha identificado al Comercio como que haya tenido un Evento de ADC diferente durante los doce (12) meses anteriores a la fecha de publicación de la primera Alerta de ADC del Evento de ADC en cuestión; y (iv) MasterCard determina que el Comercio no almacenaba Datos Confidenciales de Autenticación de la Tarjeta; o
2. Con vigencia a partir del 1 de octubre de 2015, no cobrará una FR si la entidad comprometida es un Comercio de Adquiriente de la Región de EE. UU. ubicado en la Región de EE. UU. y MasterCard determina que (i) al menos el noventa y cinco por ciento (95%) del conteo total anual de Transacciones del Comercio fue adquirido a través de

Terminales de POS Híbridas; y (ii) al menos el noventa y cinco por ciento (95%) de las Transacciones consideradas por MasterCard como dentro del alcance del Evento de ADC fueron adquiridas a través de Terminales de POS Híbridas; y (iii) MasterCard no ha identificado al Comercio como que haya tenido un Evento de ADC diferente durante los doce (12) meses anteriores a la fecha de publicación de la primera Alerta de ADC del Evento de ADC en cuestión; y (iv) MasterCard determina que el Comercio no almacenaba Datos Confidenciales de Autenticación de la Tarjeta.

A los efectos de esta subsección, el conteo total anual de las Transacciones del Comercio se determina según las Transacciones de compensación del Comercio procesadas durante los doce (12) meses anteriores a la fecha de publicación de la Alerta de ADC a través del GCMS. Las transacciones que no fueron procesadas por MasterCard se incluyen en el conteo anual de Transacciones solamente si los datos relativos a dichas Transacciones están a disposición de MasterCard. En el caso de que MasterCard no pueda determinar el conteo total anual real de las Transacciones del Comercio, MasterCard podrá aplicar su criterio para determinar un conteo total anual de Transacciones. MasterCard puede solicitar que un Adquiriente le proporcione información con dicho fin.

Todas las Regiones Excepto la Región de EE. UU.—En una investigación de Evento de ADC abierta por MasterCard el 1 de diciembre de 2014 o posteriormente, MasterCard determinará la FR de la forma establecida en la subsección mencionada arriba, de la región de EE. UU., siempre y cuando el porcentaje requerido de las Transacciones procesadas haya sido procesado a través de Terminales de POS Híbridas.

10.2.6 Recargos y/o Descalificación por No Acatamiento

Si el Cliente no acata los procedimientos establecidos en esta sección 10.2, MasterCard puede imponer un recargo de hasta USD 25.000 por día por cada día que el Cliente no acata y/o descalificar al Cliente de participar como receptor de desembolsos de reembolsos operativos y de recuperación por fraude del ADC, si dichos desembolsos están relacionados con el Evento de ADC o cualquier otro Evento de ADC, desde la fecha en que MasterCard proporciona al Cliente un aviso por escrito de dicha descalificación hasta que MasterCard determine que el Cliente ha resuelto todos los problemas de acatamiento bajo la sección 10.2.

10.2.7 Determinación Final de la Responsabilidad Financiera

Tras completar su investigación, si MasterCard determina que un Cliente tiene responsabilidad financiera en un Evento de ADC o en un Evento Potencial de ADC, MasterCard notificará al Cliente responsable de dicha determinación y, junto con dicha notificación o posterior a ella, especificará el monto de la responsabilidad financiera del Cliente del Evento ADC o del Evento Potencial de ADC.

El Cliente responsable tiene treinta (30) días calendario desde la fecha de dicha notificación del monto de responsabilidad financiera del Cliente para presentar una apelación por escrito a MasterCard, junto con cualquier documentación y/u otra información que el Cliente quiera que MasterCard considere con relación a la apelación. Solamente se considerarán las apelaciones que aleguen tanto que la determinación de responsabilidad financiera de MasterCard no se efectuó de acuerdo a las Normas como que especifiquen con particularidad

la base para dicho alegato. MasterCard establecerá un cargo no reembolsable de USD 500 por considerar y actuar sobre una solicitud de revisión de una apelación.

Si la apelación es puntual y cumple con dichos criterios, MasterCard considerará la apelación y la documentación y/u otra información presentada con la misma para determinar si la determinación definitiva de responsabilidad financiera de MasterCard se efectuó o no de acuerdo con las Normas. Las apelaciones que no sean puntuales o que no cumplan con estos criterios no serán consideradas. La decisión de MasterCard con respecto a una apelación es definitiva y no existen otros derechos de apelación internos.

Después de revisar la apelación, MasterCard notificará al cliente responsable sobre la decisión de la apelación. Si MasterCard niega o no toma acción respecto a la apelación, MasterCard debitará la cuenta MCBS del cliente responsable en la fecha que se especifique en la carta de aviso de la decisión de la apelación.

Esta sección no exime a un Cliente de las responsabilidades establecidas en las secciones 10.2.2 y 10.2.3, incluyendo la responsabilidad de presentar a MasterCard la información requerida en dichas secciones de manera continua durante el procedimiento de investigación de MasterCard. Si MasterCard determina que un Cliente tenía conocimiento o debía haber tenido conocimiento con una diligencia razonable de los documentos u otra información que se requería que el Cliente presentara a MasterCard durante el procedimiento de la investigación de MasterCard, de acuerdo con las secciones 10.2.2 ó 10.2.3, pero no lo hizo, MasterCard no tendrá en cuenta dichos documentos u otra información al tomar la decisión sobre la apelación.

10.3 MasterCard Site Data Protection (SDP) Program

NOTA: This section applies to MasterCard and Maestro Transactions.

The MasterCard Site Data Protection (SDP) Program is designed to encourage Customers, Merchants, Third Party Processors (TPPs), and Data Storage Entities (DSEs) to protect against Account data compromises. The SDP Program facilitates the identification and correction of vulnerabilities in security processes, procedures, and website configurations. For the purposes of the SDP Program, TPPs and DSEs are collectively referred to as "Service Providers" in this chapter.

An Acquirer must implement the MasterCard SDP Program by ensuring that its Merchants and Service Providers are compliant with the *Payment Card Industry Data Security Standard (PCI DSS)* and that all applicable third party-provided payment applications used by its Merchants and Service Providers are compliant with the *Payment Card Industry Payment Application Data Security Standard* (PCI PA-DSS), in accordance with the implementation schedule defined in section 10.3.1 of this manual. Going forward, the *Payment Card Industry Data Security Standard* and the *Payment Card Industry Payment Application Data Security Standard* will be components of the SDP Program; these documents set forth security Standards that MasterCard hopes will be adopted as industry standards across the payment brands.

A Customer that complies with the SDP Program requirements may qualify for a reduction, partial or total, of certain costs or assessments if the Customer, a Merchant, or a Service Provider is the source of an Account data compromise.

MasterCard has sole discretion to interpret and enforce the SDP Program Standards.

10.3.1 Payment Card Industry Data Security Standards

The *Payment Card Industry Data Security Standard* and the *Payment Card Industry Payment Application Data Security Standard* establish data security requirements. Compliance with the *Payment Card Industry Data Security Standard* is required for all Issuers, Acquirers, Digital Activity Customers, Merchants, Service Providers, and any other person or entity that a Customer permits, directly or indirectly, to store, transmit, or process Account data. MasterCard requires validation of compliance only for those entities specified in the SDP Program implementation schedule in section 10.3.4. All Merchants and Service Providers that use third party-provided payment applications must only use payment applications that are compliant with the *Payment Card Industry Payment Application Data Security Standard*, as applicable. The applicability of the PCI PA-DSS to third party-provided payment applications is defined in the *PCI PA-DSS Program Guide*.

The *Payment Card Industry Data Security Standard*, the *Payment Card Industry Payment Application Data Security Standard*, the *PCI PA-DSS Program Guide*, and other PCI Security Standards manuals are available on the PCI Security Standards Council (SSC) website at www.pcisecuritystandards.org.

10.3.2 Herramientas de Validación del Acatamiento

Según se define en el programa de implementación en la sección 10.3.4, los Comercios y Proveedores de Servicios deben validar su acatamiento de la *Norma de Seguridad de Datos de la Industria de Tarjetas de Pago* utilizando las siguientes herramientas:

Revisiones del Sitio

La revisión del sitio evalúa el acatamiento del Comercio o Proveedor de Servicios de la *Norma de Seguridad de Datos de la Industria de Tarjetas de Pago*. Las revisiones del sitio son un requisito anual para los Comercios del Nivel 1 y para los Proveedores de Servicios del Nivel 1. Los comercios pueden usar un auditor interno o un asesor independiente que MasterCard reconozca como aceptable. Los Proveedores de Servicios deben usar un asesor tercero aceptable según se define en el sitio web del Programa SDP. Las revisiones del sitio deben efectuarse de acuerdo con el manual *Payment Card Industry Security Audit Procedures*.

El *Payment Card Industry Self-assessment Questionnaire [Cuestionario de Autoevaluación de la Industria de Tarjetas de Pago]*

El *Payment Card Industry Self-assessment Questionnaire [Cuestionario de Autoevaluación de la Industria de Tarjetas de Pago]* está disponible sin costo en el sitio web del SSC de la PCI. Para estar en acatamiento, cada Comercio del nivel 2, 3 y 4, y cada Proveedor de Servicios del Nivel 2 deben generar clasificaciones aceptables anualmente.

Un Análisis de Seguridad de la Red

El análisis de seguridad de la red evalúa las medidas de seguridad que posee el sitio web. Para cumplir los requisitos de análisis de la red, todos los Comercios de Nivel 1 al 3 y todos los Proveedores de Servicios, según lo requerido por el programa de implementación deben efectuar análisis trimestralmente utilizando un proveedor que se encuentre en la lista del sitio web del SSC de la PCI. Para estar en acatamiento, se debe hacer el análisis de acuerdo con las pautas que aparecen en el manual *Payment Card Industry DSS Security Scanning Procedures*.

10.3.3 Acquirer Compliance Requirements

To ensure compliance with the MasterCard SDP Program, an Acquirer must:

- For each Level 1, Level 2, and Level 3 Merchant, submit a quarterly status report via an email message to sdp@mastercard.com using the form provided on the SDP Program website. This submission form must be completed in its entirety and may include information on:
  - The name and primary contact information of the Acquirer
  - The name of the Merchant
  - The Merchant identification number of the Merchant
  - The number of Transactions that the Acquirer processed for the Merchant during the previous 12-month period
  - The Merchant's level under the implementation schedule provided in section 10.3.4 of this manual
  - The Merchant's compliance status with its applicable compliance validation requirements
  - The Merchant's anticipated compliance validation date **or** the date on which the Merchant last validated its compliance (the "Merchant Validation Anniversary Date")
- Communicate the SDP Program requirements to each Level 1, Level 2, and Level 3 Merchant, and validate the Merchant's compliance with the *Payment Card Industry Data Security Standard* by reviewing its *Payment Card Industry Self-assessment Questionnaire* and the Reports on Compliance (ROC) that resulted from network security scans and onsite reviews of the Merchant, if applicable.
- Communicate the SDP Program requirements to each Level 1 and Level 2 Service Provider, and ensure that Merchants use only compliant Service Providers.

In submitting a quarterly SDP status report indicating that the Merchant has validated compliance within 12 months of the report submission date, the Acquirer certifies that:

1. The Merchant has, when appropriate, engaged and used the services of a data security firm(s) considered acceptable by MasterCard for onsite reviews, security scanning, or both.
2. Upon reviewing the Merchant's onsite review results, *Payment Card Industry Self-assessment Questionnaire*, or network scan reports, the Acquirer has determined that the Merchant is in compliance with the *Payment Card Industry Data Security Standard* requirements.

3. On an ongoing basis, the Acquirer will monitor the Merchant's compliance. If at any time the Acquirer finds the Merchant to be noncompliant, the Acquirer must notify the MasterCard SDP Department in writing at sdp@mastercard.com.

At its discretion and from time to time, MasterCard may also request the following information:

- Merchant principal data
- The name of any TPP or DSE that performs Transaction processing services for the Merchant's Transactions
- Whether the Merchant stores Account data

When considering whether a Merchant stores Account data, Acquirers carefully should survey each Merchant's data processing environment. Merchants that do not store Account information in a database file still may accept payment Card information via a web page and therefore store Account data temporarily in memory files. Per the MasterCard data storage definition, any temporary or permanent retention of Account data is considered to be storage. A Merchant that does not store Account data never processes the data in any form, such as in the case of a Merchant that outsources its environment to a web hosting company, or a Merchant that redirects customers to a payment page hosted by a third-party Service Provider.

10.3.4 Implementation Schedule

All onsite reviews, network security scans, and self-assessments must be conducted according to the guidelines in section 10.3.2. For purposes of the SDP Program, Service Providers in this section refer to TPPs and DSEs.

The Acquirer must ensure, with respect to each of its Merchants, that "transition" from one PCI level to another (for example, the Merchant transitions from Level 4 to Level 3 due to Transaction volume increases), that such Merchant achieves compliance with the requirements of the applicable PCI level as soon as practical, but in any event not later than one year after the date of the event that results in or causes the Merchant to transition from one PCI level to another.

All Level 1, 2, and 3 Merchants and all Service Providers that use any third party-provided payment applications must validate that each payment application used is listed on the PCI SSC website at www.pcisecuritystandards.org as compliant with the *Payment Card Industry Payment Application Data Security Standard*, as applicable. The applicability of the PCI PA-DSS to third party-provided payment applications is defined in the *PCI PA-DSS Program Guide*.

Level 1 Merchants

A Merchant that meets any one or more of the following criteria is deemed to be a Level 1 Merchant and must validate compliance with the *Payment Card Industry Data Security Standard*:

- Any Merchant that has suffered a hack or an attack that resulted in an Account data compromise,
- Any Merchant having greater than six million total combined MasterCard and Maestro transactions annually,

- Any Merchant meeting the Level 1 criteria of Visa, and
- Any Merchant that MasterCard, in its sole discretion, determines should meet the Level 1 Merchant requirements to minimize risk to the system.

To validate compliance, each Level 1 Merchant must successfully complete:

- An annual onsite assessment conducted by a PCI SSC approved Qualified Security Assessor (QSA) or internal auditor, and
- Quarterly network scans conducted by a PCI SSC Approved Scanning Vendor (ASV).

Level 1 Merchants that use internal auditors for compliance validation must ensure that primary internal auditor staff engaged in validating compliance with the *Payment Card Industry Data Security Standard* attend the PCI SSC-offered Internal Security Assessor (ISA) Program and pass the PCI SSC associated accreditation examination annually in order to continue to use internal auditors.

Level 2 Merchants

Unless deemed to be a Level 1 Merchant, the following are deemed to be a Level 2 Merchant and must validate compliance with the *Payment Card Industry Data Security Standard*:

- Any Merchant with greater than one million but less than or equal to six million total combined MasterCard and Maestro transactions annually, and
- Any Merchant meeting the Level 2 criteria of Visa.

To validate compliance, each Level 2 Merchant must successfully complete:

- An annual self-assessment, and
- Quarterly network scans conducted by a PCI SSC ASV.

Each Level 2 Merchant must ensure that staff engaged in self-assessing the Merchant's compliance with the *Payment Card Industry Data Security Standard* attend the PCI SSC-offered ISA Program and pass the associated PCI SSC accreditation examination annually in order to continue the option of self-assessment for compliance validation. Level 2 Merchants may alternatively, at their own discretion, engage a PCI SSC-approved QSA for an onsite assessment instead of performing a self-assessment.

Level 3 Merchants

Unless deemed to be a Level 1 or Level 2 Merchant, the following are deemed to be a Level 3 Merchant and must validate compliance with the *Payment Card Industry Data Security Standard*:

- Any Merchant with greater than 20,000 but less than or equal to one million total combined MasterCard and Maestro electronic commerce (e-commerce) transactions annually, and
- Any Merchant meeting the Level 3 criteria of Visa.

To validate compliance, each Level 3 Merchant must successfully complete:

- An annual self-assessment, and

- Quarterly network scans conducted by a PCI SSC ASV.

Level 4 Merchants

Any Merchant not deemed to be a Level 1, Level 2, or Level 3 Merchant is deemed to be a Level 4 Merchant. Compliance with the *Payment Card Industry Data Security Standard* is required for a Level 4 Merchant, although validation of compliance (and all other MasterCard SDP Program Acquirer requirements set forth in section 10.3.3) is optional for a Level 4 Merchant. However, a validation of compliance is strongly recommended for Acquirers with respect to each Level 4 Merchant in order to reduce the risk of Account data compromise and for an Acquirer potentially to gain a partial waiver of related assessments.

A Level 4 Merchant may validate compliance with the *Payment Card Industry Data Security Standard* by successfully completing:

- An annual self-assessment, and
- Quarterly network scans conducted by a PCI SSC ASV.

If a Level 4 Merchant has validated its compliance with the *Payment Card Industry Data Security Standard* and the *Payment Card Industry Payment Application Data Security Standard* as described in this section, the Acquirer may, at its discretion, fulfill the reporting requirements described in section 10.3.3.

Level 1 Service Providers

A Level 1 Service Provider is any TPP (regardless of volume) and any DSE that stores, transmits, or processes more than 300,000 total combined MasterCard and Maestro transactions annually.

Each Level 1 Service Provider must validate compliance with the *Payment Card Industry Data Security Standard* by successfully completing:

- An annual onsite assessment by a PCI SSC approved QSA, and
- Quarterly network scans conducted by a PCI SSC ASV.

Level 2 Service Providers

A Level 2 Service Provider is any DSE that is not deemed a Level 1 Service Provider and that stores, transmits, or processes 300,000 or less total combined MasterCard and Maestro transactions annually.

Each Level 2 Service Provider must validate compliance with the *Payment Card Industry Data Security Standard* by successfully completing:

- An annual self-assessment, and
- Quarterly network scans conducted by a PCI SSC ASV.

MasterCard has the right to audit Customer compliance with the SDP Program requirements. Noncompliance on or after the required implementation date may result in assessments described in Table 10.1.

Table 10.1—Assessments for Noncompliance with the SDP Program

Failure of the following to comply with the SDP Program mandate…	May result in an assessment of…
Classification	**Violations per calendar year**
Level 1 and Level 2 Merchants	Up to USD 25,000 for the first violation
	Up to USD 50,000 for the second violation
	Up to USD 100,000 for the third violation
	Up to USD 200,000 for the fourth violation
Level 3 Merchants	Up to USD 10,000 for the first violation
	Up to USD 20,000 for the second violation
	Up to USD 40,000 for the third violation
	Up to USD 80,000 for the fourth violation
Level 1 and Level 2 Service Providers	Up to USD 25,000 for the first violation
	Up to USD 50,000 for the second violation
	Up to USD 100,000 for the third violation
	Up to USD 200,000 for the fourth violation

Noncompliance also may result in Merchant termination, deregistration of a TPP or DSE as a Service Provider, or termination of the Acquirer as a Customer as provided in Rule 2.1.2 of the *MasterCard Rules* manual.

The Acquirer must provide compliance action plans and quarterly compliance status reports for each Level 1, Level 2, and Level 3 Merchant using the SDP Acquirer Submission and Compliance Status Form, available at http://www.mastercard.com/us/sdp/index.html or by contacting the MasterCard SDP Department at sdp@mastercard.com.

Acquirers must complete the form(s) in their entirety and submit the form(s) via email message to sdp@mastercard.com on or before the last day of the quarter, as indicated below.

For this quarter…	Submit the form(s) no later than…
1 January to 31 March	31 March
1 April to 30 June	30 June

For this quarter…	Submit the form(s) no later than…
1 July to 30 September	30 September
1 October to 31 December	31 December

Late submission or failure to submit the required form(s) may result in an additional assessment to the Acquirer as described for Category A violations in Rule 2.1.4 of the *MasterCard Rules* manual.

10.3.4.1 Enfoque Basado en el Riesgo de la DSS de la PCI de MasterCard

Un Comercio elegible de Nivel 1 o de Nivel 2 localizado fuera de la Región de EE. UU. puede usar el Enfoque Basado en el Riesgo de la DSS de la PCI de MasterCard, según el cual el Comercio:

- Valida el acatamiento con los primeros cuatro de seis objetivos importantes establecidos en el *Enfoque de Prioridad de la DSS de la PCI*, como sigue:
  - Un Comercio de Nivel 1 debe validar el acatamiento por medio de una evaluación en el sitio efectuada por un QSA aprobado por el SSC de la PCI, o realizando una evaluación en el sitio usando los recursos internos que se han capacitado y certificado por medio del Programa ISA ofrecido por el SSC de la PCI.
  - Un Comercio de Nivel 2 debe validar el acatamiento usando el Cuestionario de Auto Evaluación (SAQ) completado por los recursos internos que se han capacitado y certificado por medio del Programa ISA ofrecido por el SSC de la PCI. Como alternativa, el Comercio del Nivel 2 puede validar el acatamiento de la DSS de la PCI por medio de la evaluación en el sitio.
- Vuelve a validar anualmente el acatamiento con los objetivos importantes del uno al cuatro usando un SAQ. El SAQ debe ser completado por personal interno capacitado y certificado actualmente por medio del Programa ISA ofrecido por el SSC de la PCI.

Para calificar como en acatamiento con el Enfoque Basado en el Riesgo de la DSS de la PCI de MasterCard, un Comercio debe cumplir con cada uno de los siguientes criterios:

- El Comercio debe certificar que no almacena Datos Sensibles de Autenticación de la Tarjeta.
- De manera continua, el Comercio debe mantener totalmente separado el entorno de Transacción "Tarjeta no presente" del entorno de Transacción de "cara a cara". Una Transacción cara a cara requiere que la Tarjeta, el Tarjetahabiente y el Comercio se encuentren presentes juntos en el momento y lugar de la Transacción.
- Para un Comercio localizado en la Región de Europa, al menos el 95 por ciento del conteo total anual del Comercio de las transacciones de MasterCard y Maestro con presentación de Tarjeta debe ocurrir en Terminales de POS Híbridas.
- Para un Comercio localizado en la Región de Asia/Pacífico, Región de Canadá, Región de América Latina y el Caribe o en la Región de Medio Oriente/Africa, al menos el 75 por

ciento del conteo total anual del Comercio de las transacciones de MasterCard y de Maestro con presentación de Tarjeta debe ocurrir en Terminales de POS Híbridas.
- El Comercio no debe haber experimentado un Evento de ADC en los últimos 12 meses. A discreción de MasterCard, este y otros criterios se pueden omitir si el Comercio validó el acatamiento total de la DSS de la PCI en el momento del Evento de ADC o del Evento Potencial de ADC.
- El Comercio debe establecer y probar anualmente un plan de respuestas de incidentes de Eventos de ADC.

La información sobre el *Enfoque de Prioridad de la DSS de la PCI* está disponible en: www.pcisecuritystandards.org/education/prioritized.shtml

10.3.4.2 Programa de Exención de la Validación del Acatamiento de la DSS de la PCI de MasterCard

Un Comercio elegible de Nivel 1 o Nivel 2 puede participar en el Programa de Exención de Validación del Acatamiento de la DSS de la PCI de MasterCard (el "Programa de Exención"), que exime al Comercio del requisito de validar anualmente su acatamiento de la DSS de la PCI.

Para calificar o permanecer calificado para participar en el Programa de Exención, un funcionario del Comercio debidamente autorizado y facultado debe certificar por escrito al Adquiriente del Comercio que el Comercio ha cumplido con todo lo siguiente:

1. El Comercio validó su acatamiento con la DSS de la PCI dentro de los doce (12) meses anteriores o, de manera alterna, ha enviado a su Adquiriente, y el Adquiriente ha enviado a MasterCard, un plan de solución definido satisfactorio para MasterCard y diseñado para asegurar que el Comercio logre el acatamiento con la DSS de la PCI basado en un análisis de brecha de la DSS de la PCI;
2. El Comercio no almacena Datos Sensibles de Autenticación de la Tarjeta. El Adquiriente debe notificar a MasterCard, a través de informes de validación del acatamiento, el estado del almacenamiento por parte del Comercio de los Datos Sensibles de Autenticación de la Tarjeta;
3. El Comercio no ha sido identificado por MasterCard como un comercio que haya tenido un Evento de ADC durante los doce (12) meses anteriores;
4. El Comercio ha establecido, y prueba anualmente, un plan de respuesta a incidentes de Eventos de ADC según los requisitos de la DSS de la PCI; y
5. Al menos el 75 por ciento del conteo total anual de las Transacciones adquiridas por el Comercio de MasterCard y Maestro se procesa a través de Terminales de POS Híbridas, según se determine a partir de las transacciones del Comercio procesadas durante los doce (12) meses anteriores a través del GCMS y/o del Sistema de Mensaje Individual. Las transacciones que no fueron procesadas por MasterCard se pueden incluir en el conteo anual de Transacciones adquiridas si los datos están a disposición de MasterCard.

El Adquiriente debe conservar todos los certificados de elegibilidad del Comercio para el Programa de Exención por un mínimo de cinco (5) años. A solicitud de MasterCard, el Adquiriente debe proporcionar la certificación de elegibilidad para el Programa de Exención del Comercio y cualquier documentación y/u otra información correspondiente a dicha

certificación. El Adquiriente es responsable de garantizar que cada certificación del Programa de Exención sea veraz y exacta.

Un Comercio que no satisfaga los criterios de elegibilidad del Programa de Exención, incluidos los Comercios cuyo volumen de Transacciones proviene principalmente de los canales de aceptación de comercio electrónico y Pedido por Correo/Pedido por Teléfono (MO/TO), debe continuar validando su acatamiento a la DSS de la PCI de acuerdo a la programación de implementación de SDP de MasterCard.

Todos los Comercios deben mantener el acatamiento continuo con la DSS de la PCI independientemente de si la validación anual del acatamiento es un requisito.

10.3.4.3 Mandatory Compliance Requirements for Compromised Entities

Under the audit requirement set forth in section 10.2.2.1, the Acquirer must ensure that a detailed forensics evaluation is conducted.

At the conclusion of the forensics evaluation, MasterCard will provide a MasterCard Site Data Protection (SDP) Account Data Compromise Information Form for completion by the compromised entity itself, if the compromised entity is a TPP or DSE, or by its Acquirer, if the compromised entity is a Merchant. The form must be returned via email to pci-adc@mastercard.com within 30 calendar days of its receipt, and must include:

- The names of the QSA and the ASV that conducted the forensics evaluation, and
- The entity's current level of compliance with the *Payment Card Industry Data Security Standard*, and
- A gap analysis providing detailed steps required for the entity to achieve full compliance with the *Payment Card Industry Data Security Standard*.

As soon as practical, but no later than 60 calendar days from the conclusion of the forensics evaluation, the compromised entity or its Acquirer must provide evidence from a QSA and an ASV that the compromised entity has achieved full compliance with the *Payment Card Industry Data Security Standard*.

Such evidence (for example, a letter attesting to the entity's compliance, a compliance certificate, or a compliance status report) must be submitted to MasterCard via email to pci-adc@mastercard.com.

Failure to comply with these requirements may result in SDP noncompliance assessments as described in section 10.3.4. Any Merchant or Level 1 or Level 2 Service Provider that has suffered a confirmed Account data compromise will be automatically reclassified to become a Level 1 Merchant or a Level 1 Service Provider, respectively. All compliance validation requirements for such Level 1 entities will apply.

10.4 Connecting to MasterCard—Physical and Logical Security Requirements

Each Customer and any agent thereof must be able to demonstrate to the satisfaction of MasterCard the existence and use of meaningful physical and logical security controls for any

communications processor or other device used to connect the Customer's processing systems to the MasterCard Network (herein, "a MasterCard Network Device") and all associated components, including all hardware, software, systems, and documentation (herein collectively referred to as "Service Delivery Point Equipment") located on-site at the Customer or agent facility. Front-end communications processors include MasterCard interface processors (MIPs), network interface units (NIUs), and debit interface units (DIUs).

The controls must meet the minimum requirements described in this section, and preferably will include the recommended additional parameters.

10.4.1 Requisitos Mínimos de Seguridad

Como mínimo, el Cliente o su agente debe establecer los siguientes controles en cada instalación que albergue el Equipo del Punto de Entrega del Servicio:

1. Cada segmento de red que conecta un Dispositivo de Red de MasterCard con los sistemas de procesamiento del Cliente debe ser firmemente controlado, según sea apropiado o necesario para evitar accesos no autorizados a o desde otros segmentos de redes públicas o privadas.
2. La conectividad proporcionada por cada uno de estos segmentos de redes debe concentrarse por completo y restringirse únicamente al apoyo de las comunicaciones entre los sistemas de procesamiento del Cliente y de MasterCard.
3. El Cliente o su agente debe reemplazar cada contraseña predeterminada o proporcionada por el proveedor que esté presente en los sistemas de procesamiento del Cliente, en cada Dispositivo de Red de MasterCard y en cualquier dispositivo que proporcione conectividad entre ellos con una "contraseña segura". Una contraseña segura contiene al menos ocho caracteres, utiliza una combinación de letras, números, símbolos, puntuación, o todos, y no incluye un nombre o palabras comunes.
4. El Cliente o su agente deben efectuar revisiones periódicas regulares de todos los dispositivos y sistemas que almacenan información de la Cuenta para asegurar que el acceso se encuentre estrictamente limitado al personal del Cliente apropiado cuando "sea necesario".
5. El Cliente o su agente deben notificar a MasterCard en 30 días hábiles de cualquier cambio en el personal designado para administrar el Dispositivo de Red de MasterCard. Consulte el Apéndice B de este manual para obtener la información de contactos.
6. El Cliente o su agente deben mantener y documentar los procedimientos de auditorías adecuados para cada Dispositivo de Red de MasterCard. Los informes de la auditoría se deben conservar y estar a disposición del Cliente por al menos un año, que incluye un mínimo de 90 días en un formato electrónico de fácil recuperación.
7. El Cliente debe asegurarse de que el software implementado en cualquier sistema o dispositivo utilizado para proporcionar conectividad a la Red de MasterCard esté actualizado con todos los parches, revisiones y otras actualizaciones de seguridad adecuadas, tan pronto como se efectúe un lanzamiento.
8. Solamente debe acceder a la ubicación física del Equipo del Punto de Entrega del Servicio el personal autorizado del Cliente o su agente. El acceso de los visitantes debe estar controlado por al menos una de las siguientes medidas:

   a. Requerir que cada visitante proporcione una identificación fotográfica emitida por el gobierno antes de ingresar a la ubicación física; y/o
   b. Requerir que cada visitante sea acompañado a la ubicación física por personal autorizado del Cliente o su agente.
9. Si la ubicación física del Equipo del Punto de Entrega del Servicio proporciona acceso común a otros dispositivos o equipos, entonces el Dispositivo de Red de MasterCard debe guardarse en un gabinete que posea seguro tanto en la parte delantera como en la trasera en todo momento. Las llaves del gabinete deben guardarse en una ubicación segura.
10. El cliente o su agente deben contar con procedimientos documentados para la remoción del Equipo del Punto de Entrega del Servicio de la ubicación física.

10.4.2 Requisitos Recomendados de Seguridad Adicionales

Se recomienda encarecidamente a los Clientes y sus agentes a implementar los siguientes controles adicionales en cada instalación que contenga un Dispositivo de Red de MasterCard:

1. Disposición del Dispositivo de Red de MasterCard en una ubicación física que se encuentra rodeada de paredes desde el piso al techo.
2. Monitoreo continuo del Dispositivo de Red de MasterCard mediante cámaras y otros tipos de sistemas de vigilancia electrónicos. Los registros en video deben conservarse por un mínimo de 90 días.

10.4.3 Propiedad del Equipo del Punto de Entrega del Servicio

MasterCard es el único y exclusivo propietario de todo el Equipo del Punto de Entrega del Servicio instalado por MasterCard en el Punto de Entrega del Servicio.

Vigente a partir de la fecha de la colocación, se otorga al Cliente una Licencia no exclusiva y no transferible para usar el Equipo del Punto de Entrega del Servicio. El Cliente no puede tomar ninguna medida adversa a MasterCard con relación a su propiedad del Equipo del Punto de Entrega del Servicio.

En todo momento, el Cliente es responsable de la seguridad y del uso adecuado de todo el Equipo del Punto de Entrega del Servicio colocado en una ubicación a solicitud del Cliente y debe implementar en esa ubicación los requisitos de seguridad mínimos establecidos en esta sección 10.4. A su costo, el Cliente debe devolver inmediatamente a MasterCard todo el Equipo del Punto de Entrega del Servicio cuando MasterCard lo solicite, y sin que se le solicite, en el caso de quiebra e insolvencia.

Capítulo 11 Sistema MATCH

Este capítulo es para el personal del Adquiriente responsable de investigar e inscribir nuevos Comercios potenciales y de agregar Comercios al sistema de Alerta de MasterCard para el Control de Alto Riesgo (Comercios) (MATCH™).

11.1 Generalidades del Sistema MATCH

El sistema de Alerta para el Control de Alto Riesgo (Comercios) (MATCH™) de MasterCard está diseñado con el fin de proporcionar a los Adquirientes la oportunidad de desarrollar y revisar información de riesgo mejorada o incremental antes de celebrar un Convenio de Comercio. El MATCH es un sistema obligatorio para los Adquirientes de MasterCard. La base de datos del MATCH incluye información sobre algunos Comercios (y sus propietarios) que han sido cancelados por un Adquiriente.

Cuando un Adquiriente considera inscribir a un Comercio, el MATCH puede ayudar al Adquiriente a evaluar si el Comercio fue cancelado por otro Adquiriente debido a circunstancias que podrían afectar la decisión de adquirir para este Comercio y, si se toma la decisión de adquirir, si se debe implementar una acción o condiciones específicas en relación a la adquisición.

11.1.1 System Features

MATCH uses Customer-reported information regarding Merchants and their owners to offer Acquirers the following fraud detection features and options for assessing risk:

- Acquirers may add and search for information regarding up to five principal and associate business owners per Merchant.
- Acquirers may designate regions and countries for database searches.
- MATCH uses multiple fields to determine possible matches.
- MATCH edits specific fields of data and reduces processing delays by notifying inquiring Customers of errors as records are processed.
- MATCH supports retroactive alert processing of data residing on the database for up to 360 days.
- Acquirers determine whether they want to receive inquiry matches, and if so, the type of information that the system returns.
- MATCH processes data submitted by Acquirers once per day and provides daily detail response files.
- Acquirers may add the name of the Service Provider associated with signing the Merchant.
- Acquirers may access MATCH data in real time using MATCH Online or the Open Application Programming Interface (Open API).
- Acquirers may submit and receive bulk data using Batch and Import file operations.
- Acquirers may add and search for information regarding Merchant Universal Resource Locator (URL) website addresses.

Through direct communication with the listing Acquirer, an inquiring Acquirer may determine whether the Merchant inquired of is the same Merchant previously reported to MATCH, terminated, or inquired about within the past 360 days. The inquiring Acquirer must then determine whether additional investigation is appropriate, or if it should take other measures to address risk issues.

11.1.2 How does MATCH Search when Conducting an Inquiry?

MATCH searches the database for possible matches between the information provided in the inquiry and the following:

- Information reported and stored during the past five years
- Other inquiries during the past 360 days

MATCH searches for exact possible matches and phonetic possible matches.

NOTA: All MATCH responses reflecting that inquiry information is resident on MATCH are deemed "possible matches" because of the nature of the search mechanisms employed and the inability to report a true and exact match with absolute certainty.

NOTA: There are two types of possible matches, including a data match (for example, name-to-name, address-to-address) and a phonetic (sound-alike) match made using special software.

NOTA: For convenience only, the remainder of this manual may sometimes omit the word "possible" when referring to "possible matches" or "a possible match."

The Acquirer determines the number of phonetic matches—one to nine—that will cause a possible match to be trustworthy.

MATCH returns the first 100 responses for each inquiry submitted by an Acquirer. MATCH returns all terminated Merchant MATCH responses regardless of the number of possible matches.

11.1.2.1 Posibles Cotejos Retroactivos

Si en la información en la consulta original se encuentran posibles concordancias nuevas de un Comercio o un registro de consulta en la base de datos del MATCH agregada desde que fue presentada la consulta original y esta información no ha sido comunicada anteriormente al Adquiriente al menos una vez en los últimos 360 días, el sistema devuelve una respuesta de posible concordancia **retroactiva**.

11.1.2.2 Posibles Cotejos Exactos

El MATCH encuentra un posible cotejo exacto cuando los datos en un registro de consulta concuerdan con los datos en el sistema MATCH, letra por letra, número por número o ambos. Un cotejo exacto con cualquiera de los siguientes datos resultará en una respuesta de posible cotejo de MasterCard:

Tabla 11.1—Criterios de la Posible Concordancia Exacta

Campo	+	Campo	+	Campo	=	Match [Concordancia]
Nombre del Comercio					=	√
Nombre Bajo el Cual Opera el Comercio (DBA)					=	√
Número de Teléfono (Comercio)					=	√
Número de Teléfono Alternativo (Comercio)					=	√
Identificación Tributaria Nacional del Comercio	+	Country			=	√
Identificación Tributaria Estatal del Comercio	+	Estado			=	√
Dirección Física del Comercio	+	Ciudad	+	Estado[4]	=	√
Dirección Física del Comercio	+	Ciudad	+	País[5]	=	√
Dirección del Sitio Web del URL del Comercio	+	Ciudad	+	Country	=	√
Nombre del Propietario Principal (PO)	+	Apellido			=	√
Número de Teléfono del PO					=	√
Número de Teléfono Alternativo (PO)					=	√
Número de Seguro Social del Propietario Principal					=	√
Identificación Nacional del Propietario Principal					=	√

[4] Si el país es EE. UU.
[5] Si el país no es EE. UU.

Campo	+	Campo	+	Campo	=	Match [Concordancia]
PO Street Address [Dirección del Propietario Principal] (renglones 1 y 2)	+	PO City [Ciudad del Propietario Principal]	+	Estado del Propietario Principal[4]	=	√
PO Street Address [Dirección del Propietario Principal] (renglones 1 y 2)	+	PO City [Ciudad del Propietario Principal]	+	País del Propietario Principal[5]	=	√
PO Driver's License (DL) Number [Número de la Licencia de Conducir (DL) del Propietario Principal]	+	Estado de la Licencia de Conducir[4]			=	√
PO Driver's License Number [Número de la Licencia de Conducir (DL) del Propietario Principal]	+	País de la Licencia de Conducir[5]			=	√

NOTA: El MATCH usa la Dirección, Ciudad y el Estado si el país del Comercio es EE. UU.; de otro modo se usa la Dirección, Ciudad y el País.

NOTA: Los adquirientes deben llenar el campo de Dirección del Sitio Web del URL del Comercio al realizar una consulta de un Comercio de comercio electrónico.

11.1.2.3 Posibles Cotejos Fonéticos

El sistema MATCH convierte ciertos datos alfabéticos, tales como el Nombre y Apellido del Propietario Principal del Comercio a un código fonético. El código fonético genera cotejos para palabras que suenen parecido, tales como "Easy" y "EZ". La característica del cotejo fonético del sistema también coteja nombres que no son necesariamente un cotejo fonético pero que pueden diferenciarse debido a un error tipográfico tal como "Rogers" y "Rokers", o una variación ortográfica como "Lee," "Li" y "Leigh".

El MATCH evalúa los siguientes datos para determinar un posible cotejo fonético.

Tabla 11.2—Criterios de la Posible Concordancia Fonética

Campo	+	Campo	+	Campo	=	Match [Concordancia]
Nombre del Comercio					=	√
Nombre Bajo el Cual Opera el Comercio (DBA)					=	√
Dirección Física del Comercio	+	Ciudad	+	Estado	=	√
Dirección Física del Comercio	+	Ciudad	+	País	=	√
Nombre del Propietario Principal (PO)	+	Apellido			=	√
PO Street Address [Dirección del Propietario Principal] (renglones 1 y 2)	+	PO City [Ciudad del Propietario Principal]	+	Estado del Propietario Principal[6]	=	√
PO Street Address [Dirección del Propietario Principal] (renglones 1 y 2)	+	PO City [Ciudad del Propietario Principal]	+	País del Propietario Principal[7]	=	√

NOTA: El MATCH usa la Dirección, Ciudad y el Estado si el país del Comercio es EE. UU.; de otro modo se usa la Dirección, Ciudad y el País.

11.2 Normas del Sistema MATCH

MasterCard exige que todos los Adquirientes con actividades de Comercio usen el MATCH. El usarlo significa que deben:

- Agregar la información sobre un Comercio que ha sido cancelado mientras y debido a una circunstancia existente (Consulte la sección 11.2.2), e
- Investigar contra la base de datos del MATCH.

[6] Si el país es EE. UU.
[7] Si el país no es EE. UU.
[8] Se cobra globalmente a los adquirientes un cargo anual de uso del MATCH de US$5.000. Además, se cobra a los Adquirientes un cargo por consulta al MATCH (por número ICA/Identificación del Miembro) por cada consulta al MATCH.

Los clientes deben actuar diligente y razonablemente y de buena fe para acatar las Normas del MATCH.

11.2.1 Certification

Each Acquirer that conducts Merchant acquiring Activity must be certified by MasterCard to use MATCH because it is a mandatory system. An Acquirer that does not comply with these requirements may be assessed for noncompliance, as described in this chapter.

Certification is the process by which MasterCard connects an Acquirer to the MATCH system, so that the Acquirer may send and receive MATCH records to and from MasterCard. To be certified for MATCH usage, Acquirers must request access for each Member ID/ICA number under which acquiring Activity is conducted.

NOTA: An Acquirer that conducts Merchant acquiring Activity under a Member ID/ICA number that does not have access to the MATCH system is not considered certified.

An Acquirer that is not MATCH-certified is subject to noncompliance assessments as described in Table 11.3.

11.2.2 Cuándo Agregar un Comercio al sistema MATCH

Si el Adquiriente o el Comercio actúa para cancelar la relación de adquisición (como dar aviso de cancelación) y, en el momento de ese acto, el Adquiriente tiene motivos para creer que existe una condición descrita en la Tabla 11.4, entonces el Adquiriente debe agregar la información requerida al MATCH dentro de cinco días calendario, lo que sea primero de:

1. Una decisión por parte del Adquiriente para cancelar la relación de adquisición, independiente de la fecha de vigencia de la cancelación, o
2. El recibo del Adquiriente de un aviso del Comercio o en su nombre de la decisión de cancelar la relación adquiriente, independientemente de la fecha de vigencia de la cancelación.

Los adquirientes deben actuar diligentemente, razonablemente y de buena fe para acatar los requisitos del sistema MATCH.

Los adquirientes no pueden usar o amenazar con usar el MATCH como una herramienta de cobro por actividad discrecional de Comercios de poca importancia. Uno de los códigos de motivo definidos en la Tabla 11.4 debe ser cumplido o sospechado (en el momento de tomar la decisión de cancelación) para justificar el agregar un Comercio. Los adquirientes que utilicen o amenacen con utilizar el MATCH como una herramienta de cobro para actividades discrecionales de Comercios de poca importancia están sujetos a recargos por no acatamiento, según se describe en Tabla 11.3.

Un Adquiriente que no ingresa un Comercio en el MATCH está sujeto a un recargo por no acatamiento, y puede estar sujeto a un fallo desfavorable en un caso de acatamiento presentado por un Adquiriente posterior de ese Comercio.

11.2.3 Cómo Hacer una Consulta sobre un Comercio

Un Adquiriente debe comprobar el MATCH **antes** de firmar un convenio con un Comercio de acuerdo con la sección 7.1 de este manual.

Un Adquiriente que celebra un Convenio de Comercio sin antes consultar al MATCH sobre el Comercio puede estar sujeto a un fallo desfavorable en un caso de acatamiento presentado por un Adquiriente posterior de ese Comercio.

Los adquirientes deberán realizar consultas bajo el Número de Identificación del Miembro/ICA apropiado para informar los motivos de acatamiento. Si un Adquiriente no realiza la consulta bajo la Identificación del Miembro/Número ICA adecuado (es decir, la Identificación del Miembro/Número ICA que realmente procesa para el Comercio), MasterCard puede considerar que el Adquiriente está en estado de no acatamiento y podrá imponer un recargo.

El no acatamiento del requisito de agregar un Comercio cancelado o hacer una consulta sobre un Comercio puede resultar en recargos por no acatamiento según se describe en la Tabla 11.3.

11.2.4 Recargos por No Acatamiento del sistema MATCH

Los adquirientes que no acaten los requisitos de certificación o uso del MATCH (agregar o hacer consultas sobre Comercios, utilizar o amenazar con utilizarlo como una herramienta de cobro para la actividad discrecional de Comercio de poca importancia) están sujetos a un recargo por no acatamiento tal como se describe en la Tabla 11.3. A su discreción, MasterCard determinará si el Adquiriente está en acatamiento del reglamento. Si se considera conveniente, MasterCard informará al gerente principal del Adquiriente de los casos de no acatamiento y de los recargos resultantes del no acatamiento.

Tabla 11.3—Recargos por No Acatamiento

Motivo	Recargo
Si no se certifica para el uso del MATCH bajo cada número ICA/Identificación del Miembro utilizado para la Actividad de adquisición del Comercio	Hasta USD 10.000 por mes hasta la certificación del Adquiriente
Si no se consulta al MATCH antes de firmar el Convenio de Comercio	Hasta USD 5.000 por cada caso de no acatamiento
Si no se agrega a un Comercio cancelado al MATCH	Hasta USD 5.000 por mes por cada caso de no acatamiento
Usar o amenazar con usar el MATCH como una herramienta de cobro para actividad discrecional de Comercios de poca importancia	Hasta USD 5.000 por cada caso de no acatamiento

11.2.5 Excepciones a las Normas del Sistema MATCH

Por cualquier excepción a estas Normas del MATCH, envíe una solicitud por escrito a la dirección de Control de Fraude del Comercio proporcionada en la sección Servicios de Seguridad y Riesgo del Apéndice B.

11.2.6 MATCH Record Retention

An Acquirer should retain all MATCH records returned by MasterCard to substantiate that the Acquirer complied with the required procedures. MasterCard recommends that the Acquirer retain these records in a manner that allows for easy retrieval.

Merchant records remain on the MATCH system for five years. Each month, MATCH automatically purges any Merchant information that has been in the database for five years.

NOTA: The MATCH system database stores inquiry records for 360 days.

11.3 Comercios Listados por MasterCard

Un listado de Comercios puede propiciar una consulta o una consulta adicional de un Adquiriente sobre un Comercio. Si los datos de consulta del MATCH cotejan con los datos en el archivo del MATCH, ya sea por un cotejo exacto o por cotejo fonético, MasterCard generará un registro de respuesta. El Número ICA/Identificación de Miembro 1996 en un registro de respuesta, junto con uno de los códigos de motivo del MATCH listados en la Tabla 11.6 indica que el registro de consulta concuerda con un Comercio Listado en MasterCard.

NOTA: Un valor de 1996 en el campo del Número de Referencia de MasterCard de un registro de respuesta indica que una consulta posiblemente resultó en una concordancia con un registro de Comercio sospechoso.

Los adquirientes que reciben una respuesta de posible concordancia con el Número ICA/Identificación de Miembro 1996 en el campo Número de Referencia de MasterCard pueden comunicarse con el personal del Departamento de Control de Fraude del Comercio según se describe en la sección Servicios de Riesgo y Seguridad del Apéndice B.

11.3.1 Comercios Sospechosos

El MATCH también contiene datos sobre Comercios y sus propietarios clasificados como sospechosos por el personal de Control de Fraude del Comercio. Estos Comercios y propietarios aparecen listados como Comercios sospechosos debido a que MasterCard audita al Comercio en acatamiento al reglamento.

Un listado de Comercios sospechosos puede propiciar una consulta o una consulta adicional de un Adquiriente sobre un Comercio. Si los datos de consulta del MATCH cotejan con los datos en el archivo del MATCH, ya sea por un cotejo exacto o por cotejo fonético, MasterCard generará un registro de respuesta. La Identificación del Miembro/Número ICA 1996 en un registro de respuesta, junto con un código de motivo del MATCH 00, indica que el registro de consulta concuerda con un ingreso de Comercio sospechoso.

11.4 Eliminación de Comercios del MATCH

MasterCard puede eliminar a un Comercio que se encuentra en la lista del MATCH por los siguientes motivos:

- El Adquiriente informa a MasterCard que el Adquiriente agregó el Comercio al MATCH por error.
- El Comercio fue incluido en la lista por el código de motivo 12 (No Acatamiento de la *Norma de Seguridad de Datos de la Industria de Tarjetas de Pago*) y el Adquiriente confirma que el Comercio acata la *Norma de Seguridad de Datos de la Industria de Tarjetas de Pago*. Para eliminar un Comercio con código de motivo de MATCH 12 de la lista del MATCH, el Adquiriente debe presentar por escrito al Control de Fraude del Comercio una solicitud con el membrete del Adquiriente. Dicha solicitud debe incluir la siguiente información:

  1. Número de Identificación del Adquiriente
  2. Número de Identificación del Comercio
  3. Nombre del Comercio
  4. Nombre Bajo el Cual Opera el Comercio (DBA)
  5. Dirección del Negocio
     a. Dirección
     b. Ciudad
     c. Estado
     d. País
     e. Código postal
  6. Datos del Propietario Principal (PO)
     a. Nombre y Apellido del Propietario Principal
     b. País de Residencia del PO

     Consulte la sección B.2 del Apéndice B de este manual para obtener la información de contactos del Control de Fraude del Comercio.

     Toda solicitud relacionada con un Comercio listado para el código de motivo 12 debe contener:

     – La declaración del Adquiriente de que el Comercio está en acatamiento de la *Norma de Seguridad de Datos de la Industria de Tarjetas de Pago*, y
     – Una carta o un certificado de validación de un examinador forense certificado de MasterCard, que certifica que el Comercio acata la *Norma de Seguridad de Datos de la Industria de Tarjetas de Pago*.

     Si un Adquiriente no está dispuesto o no puede presentar una solicitud a MasterCard con respecto a la eliminación de un Comercio de un listado del MATCH debido a que el Comercio logró el acatamiento de la *Norma de Seguridad de Datos de la Industria de Tarjetas de Pago*, el Comercio por sí mismo puede presentar una solicitud a MasterCard por este motivo. El Comercio debe seguir el mismo proceso

que se describió anteriormente para los Adquirientes que presentan una solicitud de eliminación del MATCH.

11.5 Códigos de Motivo del MATCH

Los códigos de motivo del MATCH identifican si el Adquiriente o MasterCard agregaron un Comercio al sistema MATCH y el motivo de su inclusión en dicha lista.

11.5.1 Códigos de Motivo para los Comercios Listados por el Adquiriente

Los códigos de motivo a continuación indican el motivo por el que el Adquiriente comunicó la cancelación de un Comercio al MATCH.

Tabla 11.4—Códigos de Motivo para el Listado del MATCH Usados por los Adquirientes

Código de Motivo del MATCH	Descripción
01	***Compromiso de los Datos de la Cuenta*** Un incidente que da como resultado, de manera directa o indirecta, el acceso no autorizado a datos de la Cuenta o la divulgación de los mismos.
02	***Punto de Compra Común (CPP)*** Los datos de la cuenta son robados en el Comercio y luego usados para compras fraudulentas en otras ubicaciones del Comercio.
03	***Lavado de Dinero*** El Comercio participó en la actividad de lavado de dinero. Lavado de dinero significa que un Comercio presentó a sus Adquirientes registros de Transacciones que no eran Transacciones válidas por ventas de bienes o servicios entre ese Comercio y un Tarjetahabiente legítimo.
04	***Exceso de Contracargos*** Con respecto a un Comercio informado por un Adquiriente de MasterCard, el número de contracargos de MasterCard en cualquier mes individual excedió el 1% del número de Transacciones de ventas de MasterCard en ese mes, y el total de esos contracargos fue de US $5.000 o más. Con respecto a un comercio sobre el que ha informado un Adquiriente de American Express (números ICA del 102 al 125), el comercio excedió los márgenes de contracargo de American Express, según lo determina American Express.

Código de Motivo del MATCH	Descripción
05	***Fraude Excesivo*** El Comercio realizó Transacciones fraudulentas de cualquier tipo (falsificación o de otra forma) que cumplieron o sobrepasaron la siguiente Norma de presentación de informes mínima: la relación del volumen en dólares del fraude sobre las ventas del Comercio fue del 8% o mayor en un mes calendario, y el Comercio efectuó 10 o más Transacciones fraudulentas por un total de US$5.000 o más en ese mes calendario.
06	***Reservado para Uso Futuro***
07	***Condena por Fraude*** Hubo una condena criminal por fraude de un dueño o socio principal del Comercio.
08	***Programa de Auditoría del Comercio Sospechoso de MasterCard*** Se determinó que el Comercio era un Comercio Sospechoso de conformidad con los criterios establecidos en el Programa de Auditoría del Comercio Sospechoso de MasterCard (consulte la sección 8.4 de este manual).
09	***Quiebra/Liquidación/Insolvencia*** El Comercio no pudo o probablemente no pueda cumplir con sus obligaciones financieras.
10	***Violación de las Normas*** Con respecto a un Comercio sobre el que ha informado un Adquiriente de MasterCard, el Comercio violaba una o más Normas que describen los procedimientos que debe emplear el Comercio en las Transacciones en las que se usan Tarjetas, incluyendo, entre otras, las Normas de aceptación de todas las Tarjetas, la exhibición de las Marcas, los cargos a los Tarjetahabientes, las restricciones de monto mínimo/máximo de la Transacción y las Transacciones prohibidas establecidas en el Capítulo 5 del manual *Reglamento de MasterCard*. Con respecto a un comercio sobre el que ha informado un adquiriente de American Express (números ICA del 102 al 125), el comercio estaba en violación de uno o más estatutos, reglamentos, reglas de operación y políticas de American Express que establecen los procedimientos que el comercio debe utilizar en las transacciones en las cuales se usan las tarjetas American Express.
11	***Confabulación del Comercio*** El Comercio participó en una actividad de confabulación fraudulenta.

Código de Motivo del MATCH	Descripción
12	**No acatamiento de la *Norma de Seguridad de los Datos de la PCI*** El Comercio no acató los requisitos de la *Norma de Seguridad de los Datos de la Industria de Tarjetas de Pago (PCI)*.
13	***Transacciones Ilegales*** El Comercio estuvo involucrado en Transacciones ilegales.
14	***Robo de Identidad*** El Adquiriente tiene motivos para creer que la identidad del Comercio listado o la de su/s propietario/s principales fue asumida ilegalmente con el propósito de participar de forma ilegal en un Convenio de Comercio.

11.5.2 Reason Codes for Merchants Listed by MasterCard

The following MATCH reason codes and descriptions apply to those Merchants listed following evaluation by the Merchant Fraud Control staff.

Table 11.6—MATCH Reason Codes and Descriptions

MATCH Reason Code	Description
00	***Questionable Merchant/Under Investigation*** A Merchant that is the subject of an audit with respect to the Standards. MasterCard currently conducts special Merchant audits for excessive fraud-to-sales ratios, excessive chargebacks, counterfeit activity, or collusive or otherwise fraudulent Merchant activity.
20	***MasterCard Questionable Merchant Audit Program*** A Merchant that MasterCard has determined to be a Questionable Merchant as per the criteria set forth in the MasterCard Questionable Merchant Audit Program (refer to section 8.4 of this manual).
21	***Non-face-to-face Adult Content and Services Special Merchant*** A non-face-to-face adult content and services Merchant that MasterCard has determined to have violated MasterCard excessive chargeback Standards.

MATCH Reason Code	Description
22	***Excessive Chargeback Merchant*** A Merchant that MasterCard has determined to have violated the MasterCard Excessive Chargeback Program and is not a non-face-to-face adult content and services Merchant.
23	***Merchant Collusion*** The Merchant participated in fraudulent collusive activity, as determined by the Acquirer by any means, including data reporting, criminal conviction, law enforcement investigation, or as determined by MasterCard.
24	***Illegal Transactions*** The Merchant was engaged in illegal Transactions.

11.6 Cómo Solicitar el Acceso y Utilizar el MATCH

Los clientes pueden solicitar acceso al MATCH por medio de la Tienda MasterCard Connect en MasterCard Connect™.

Para obtener información sobre los registros del MATCH, sobre cómo acceder y navegar en el sistema MATCH, realizar consultas, y agregar, modificar o eliminar información del Comercio, consulte el *MATCH User Manual*, disponible en el producto Publications [Publicaciones] en MasterCard Connect™.

Para obtener información técnica sobre el uso del MATCH, consulte el *MATCH User Manual*, disponible en el producto Publications [Publicaciones] en MasterCard Connect™.

Para obtener información sobre los informes del MATCH, consulte el *MATCH User Manual*.

11.7 Legal Notice

The MasterCard MATCH system and data are proprietary and confidential to MasterCard International and its licensed Customers.

A Customer may use MATCH solely for the purpose of developing enhanced or incremental risk information before entering into a Merchant Agreement; any other use is prohibited.

The Standards in Chapter 11 of the MasterCard *Security Rules and Procedures* set forth Customer rights and obligations pertaining to access to and use of MATCH. The Standards require, among other things, that an Acquirer conduct an inquiry before acquiring MasterCard-branded Transactions from a Merchant and that an Acquirer report information

pertaining to a Merchant that has been terminated for any one or more of a specified number of reasons. The Standards do not require an Acquirer to take any action or any specific action after receiving a response record and do not require that an Acquirer provide any information to or otherwise cooperate with any other Acquirer. MATCH may enable an Acquirer to develop enhanced or incremental risk information concerning a Merchant, but does not itself provide risk information. The Acquirer itself must determine whether the Merchant that is the subject of a "possible match" response is the same Merchant that the Acquirer conducted an inquiry about. A "possible match" response to an inquiry does not mean or suggest that a Merchant is a poor risk or greater risk than any other Merchant. A Customer itself must determine whether a Merchant poses a risk and, if so, the nature of such risk.

MasterCard does not verify, otherwise confirm, or ask for confirmation of either the basis for or accuracy of any information that is reported to or listed in MATCH. MATCH may include incorrect, inaccurate, and incomplete information as well as information that should not have been reported. It is possible that facts and circumstances giving rise to a MATCH system report may be subject to interpretation and dispute.

Use of MATCH is "Activity", as such term is defined in the Definitions portion of the *MasterCard Rules*. MATCH is a part of "Systems", as such term is defined in MasterCard Rule 2.3 (Indemnity and Limitation of Liability). A Customer that directly or indirectly has access to or use of MATCH is an "Indemnifying Customer," as such term is defined in MasterCard Rule 2.3. A Customer's direct or indirect access to or use of MATCH is Activity of that Customer and subject to the terms of MasterCard Rule 2.3.

Capítulo 12 Normas de la Presentación de Informes al Sistema para Evitar el Fraude con Eficacia (SAFE)

Este capítulo trata sobre la información de datos de fraude a MasterCard mediante SAFE OnLine. Además esta sección proporciona una descripción del Programa de Acatamiento al SAFE.

12.1 Generalidades del SAFE

MasterCard exige a todos los Emisores que informen las Transacciones fraudulentas a MasterCard usando el Sistema para Evitar el Fraude con Eficacia (SAFE). Cada Emisor debe asegurarse de que la información de Transacción enviada a MasterCard a través del SAFE sea precisa y que se entregue en forma oportuna. MasterCard ha establecido controles de calidad de los datos para controlar la información de Transacción que un Emisor envía al SAFE. El SAFE no permite a un Emisor informar créditos fraudulentos (reembolsos) en una Cuenta o autorizaciones que el Emisor rechazó debido a una sospecha de posible fraude.

Un emisor no debe informar las siguientes transacciones al SAFE:

- Créditos fraudulentos (reembolsos) en una Cuenta
- Autorizaciones que el Emisor rechazó debido a una sospecha de posible fraude
- Una Transacción disputada por el Tarjetahabiente como fraudulenta, pero que el Emisor determina que fue realizada por el Tarjetahabiente o por una persona de quien el Tarjetahabiente es responsable en cuestiones financieras, y las credenciales del Tarjetahabiente y la Tarjeta o el Dispositivo de Acceso no fueron robados o extraviados. Esto incluye, entre otros, las situaciones donde:
  - El Tarjetahabiente no pudo obtener un reembolso del Comercio:
  - Una persona, de quien el Tarjetahabiente es responsable en cuestiones financieras, involucrado en una Transacción sin el conocimiento o el consentimiento del Tarjetahabiente; o
  - El Tarjetahabiente también es el Comercio o es empleado del Comercio.

Dichas Transacciones se denominan «remordimiento del comprador» o «fraude amistoso» y se consideran disputas o problemas de crédito del Tarjetahabiente en lugar de Transacciones fraudulentas.

12.2 Normas de la Presentación de Informes de Fraude al SAFE

Un Emisor debe usar el SAFE para la presentación mensual de informes de todos los tipos de Transacciones, incluyendo las Transacciones contracargadas por un motivo relacionado con fraude y las Transacciones para las cuales las pérdidas por fraude se recuperaron por un medio diferente a un contracargo:

1. Todas las Transacciones fraudulentas del Punto de Venta (POS) de MasterCard;
2. Todas las Transacciones fraudulentas de POS de Maestro procesadas mediante el Sistema de Intercambio y las Transacciones fraudulentas de POS de Maestro dentro de Europa y entre países de Europa no procesadas mediante el Sistema de Intercambio; y
3. Todas las Transacciones fraudulentas de ATM.

El Emisor debe identificar cada Transacción fraudulenta comunicada al SAFE utilizando el código de motivo del SAFE correspondiente, según se establece en la sección 12.3.

Un Emisor, sin casos de Transacciones fraudulentas para comunicar durante un período relevante de presentación de informes pertinente, debe presentar un Registro de Informe Negativo de Fraude (FDN) a fines del mes del informe.

NOTA: Un Emisor puede presentar un Registro de FDN entre el primer día y el último día del mes. Para obtener información sobre cómo presentar dicho informe, consulte el Capítulo 1 de la *Guía del Usuario de los Productos del SAFE*.

12.2.1 Transacciones de Pago a Distancia Digital Garantizado.

El emisor debe comunicar al SAFE cada Transacción de Pago a Distancia Digital Garantizado identificada como fraudulenta usando el código de motivo del SAFE 05 (Fraude por Usurpación de Cuenta). Para obtener información sobre los requisitos de identificación de las Transacciones de Pago a Distancia Digital Garantizado, consulte el Apéndice E de la *Guía de Contracargo*.

12.3 Códigos de Motivo del SAFE

Los siguientes códigos de motivo del SAFE deben ser utilizados por los Emisores para indicar el motivo por el cual Emisor informó una Transacción fraudulenta a través del SAFE.

Tabla 12.1—Códigos de Motivo del Listado del SAFE Usados por los Emisores

Código	Descripción
00	**Fraude con Tarjeta Extraviada**—Una Transacción fraudulenta que ocurre mediante el uso de una Tarjeta extraviada u otro Dispositivo de Acceso (u otro instrumento para el acceso a una Cuenta, por ejemplo, los cheques de conveniencia y de transferencia de saldo) sin la autorización real, implícita o aparente del Tarjetahabiente.
01	**Fraude con Tarjeta Robada**—Una Transacción fraudulenta que ocurre mediante el uso de una Tarjeta robada u otro Dispositivo de Acceso (u otro instrumento para el acceso a una Cuenta, por ejemplo, los cheques de conveniencia y de transferencia de saldo) sin la autorización real, implícita o aparente del Tarjetahabiente.
02	**Tarjeta Emitida Nunca Recibida**—La interceptación y uso de una Tarjeta u otro Dispositivo de Acceso (u otro instrumento de acceso a una Cuenta, por ejemplo, los cheques de conveniencia y de transferencia de saldo) antes de ser recibido por el Tarjetahabiente, por una persona sin la autorización real, implícita o aparente del Tarjetahabiente.
03	**Solicitud Fraudulenta**—Una Transacción fraudulenta que ocurre mediante el uso de una Tarjeta u otro Dispositivo de Acceso obtenido con una solicitud que contiene un nombre falso u otra información de identificación falsa.

Código	Descripción
04	**Fraude con Tarjeta Falsificada**—El uso de una Tarjeta u otro Dispositivo de Acceso alterado o reproducido ilegalmente (u otro instrumento para acceder a una Cuenta, por ejemplo, los cheques de conveniencia y de transferencia de saldo) incluyendo la réplica o alteración de la banda magnética o grabado al relieve.
05	**Fraude por Usurpación de Cuenta**—Una Cuenta existente de crédito o débito que se usa sin la autorización real, implícita o aparente del Tarjetahabiente, por una persona que obtiene acceso y utiliza la Cuenta por un medio no autorizado, como un cambio de dirección o la solicitud de reemisión de una Tarjeta u otro Dispositivo de Acceso (u otro instrumento para acceder a una Cuenta, por ejemplo, cheques de conveniencia y de transferencia de saldo) pero que no son Tarjetas extraviadas o robadas.
06	**Fraude Sin Presentación de Tarjeta**—Una Transacción fraudulenta que ocurre mediante el uso de la información de una Cuenta de crédito o débito, que incluye información de una seudocuenta sin involucrar la Tarjeta u otro Dispositivo de Acceso, por medio de teléfono, correo, Internet u otro medio electrónico sin la autorización real, implícita o aparente del Tarjetahabiente.
07	**Fraude por Impresiones Múltiples**—Una Transacción fraudulenta que ocurre con una Tarjeta de crédito o de débito donde el Comercio, tras haber completado una Transacción legítima cara a cara, deposita una o más Transacciones adicionales sin la autoridad real, implícita o aparente del Tarjetahabiente. Por ejemplo, el Comercio hace varias impresiones de una Tarjeta en los juegos de formularios de papel o produce recibos de la Terminal de POS tras recibir aprobaciones de autorización adicionales por lectura de Tarjeta en línea o fuera de línea.
51	**Comercio Confabulado en Bust-out**—Un Tarjetahabiente que efectúa Transacciones en confabulación con un Comercio tal como se define en el Programa de Auditoría del Comercio Sospechoso de MasterCard.

12.4 Exactitud e Integridad de los Datos

El emisor es responsable de presentar las Transacciones fraudulentas con exactitud mediante la herramienta SAFE. MasterCard coteja la información del SAFE presentada con los registros de autorización y compensación correspondientes para asegurar la exactitud de los datos.

12.5 Puntualidad en la Presentación de Informes de las Transacciones de MasterCard y de Debit MasterCard

Para las transacciones de MasterCard® y Debit MasterCard®, MasterCard ha establecido tres escalas para monitorizar la puntualidad en la presentación de informes al SAFE según el tipo de fraude.

Tabla 12.2—Clasificación de Fraude por Escala

Fraude de Escala I	Fraude de Escala II	Fraude de Escala III
Código de Motivo 00 (Tarjeta Extraviada)	Código de Motivo 06 (Sin Presentación de Tarjeta)	Código de Motivo 03 (Solicitud Fraudulenta)
Código de Motivo 01 (Tarjeta Robada)		Código de Motivo 05 (Usurpación de Cuenta)
Código de Motivo 02 (Tarjeta Emitida Nunca Recibida)		Código de Motivo 07 (Impresión Múltiple)
Código de Motivo 04 (Fraude con Tarjeta Falsificada)		

A los efectos del programa SAFE, los siguientes términos tienen los significados que se establecen a continuación:

1. "Transacción de Escala I" se refiere a una Transacción que se identifica adecuadamente utilizando el código de motivo de mensaje del SAFE 00 (Fraude por Extravío), 01 (Fraude por Robo), 02 (Tarjeta Emitida Nunca Recibida) o 04 (Fraude con Tarjeta Falsificada).
2. "Transacción de Escala II" se refiere a una Transacción que se identifica adecuadamente utilizando el código de motivo de mensaje del SAFE 06 (Fraude Sin Presentación de Tarjeta).
3. "Transacción de Escala III" se refiere a una Transacción que se identifica adecuadamente utilizando el código de motivo de mensaje del SAFE 03 (Solicitud Fraudulenta), 05 (Fraude por Usurpación de Cuenta), o 07 (Fraude por Impresiones Múltiples).

12.5.1 Requisitos de la Presentación de Informes de Nivel I

Un Emisor debe informar al menos el 80% de las Transacciones de Nivel I al SAFE dentro de los 60 días de la fecha de la Transacción **o** de los 30 días de la fecha de la notificación del Tarjetahabiente **o** de los 60 días a partir de la fecha del primer contracargo, a menos que las Normas requieran que el Emisor informe la Transacción al SAFE antes de que ocurra un contracargo.

12.5.2 Requisitos de la Presentación de Informes de Nivel II

Un Emisor debe informar al menos el 65% de las Transacciones de Nivel II al SAFE dentro de los 60 días a partir de la fecha de la Transacción **o** de los 30 días de la fecha de la notificación del Tarjetahabiente **o** de los 60 días a partir de la fecha del primer contracargo, a menos que las Normas requieran que el Emisor informe la Transacción al SAFE antes de que ocurra un contracargo.

12.5.3 Requisitos de la Presentación de Informes de Nivel III

Un Emisor debe informar las Transacciones de Nivel III al SAFE dentro de los 30 días de la fecha de notificación al Tarjetahabiente.

12.6 Puntualidad en la Presentación de Informes de las Transacciones de Maestro

Todas las Transacciones fraudulentas de POS de Maestro procesadas a través del Sistema de Intercambio, las Transacciones fraudulentas de POS de Maestro dentro de Europa y entre países de Europa no procesadas a través del Sistema de Intercambio y las Transacciones fraudulentas de ATM de Maestro deben informarse al SAFE. El Emisor debe informar al menos el 80% de todas las Transacciones fraudulentas al SAFE dentro de los 60 días posteriores a la fecha de la Transacción o 30 días a partir de la fecha de la notificación del Tarjetahabiente.

12.7 Puntualidad en la Presentación de Informes de las Transacciones de Cirrus

Una Transacción de Cirrus® es una transacción de ATM que tiene lugar mediante el uso de una Tarjeta que contiene la(s) Marca(s) Cirrus pero ninguna otra Marca o marca(s) de Visa y que se procesa a través del Sistema de Intercambio. El Emisor debe informar al menos el 80% de todas las Transacciones fraudulentas de Cirrus al SAFE dentro de los 90 días de la fecha de descubrimiento o de los 90 días de la fecha de la notificación del Tarjetahabiente, lo que ocurra primero.

12.8 Transacciones de Bienes Digitales

Un Emisor no debe informar una Transacción de comercio electrónico no fraudulenta de USD 25 o menos (o su equivalente en moneda local) para la compra de Bienes Digitales a través del SAFE. Un Emisor que comunica dicha Transacción a través del SAFE estará sujeto a recargos por no acatamiento de las Normas de presentación de informes al SAFE.

12.9 Fraud-related Chargebacks

An Issuer must report all fraudulent Transactions to SAFE, notwithstanding the status of the Account or the reason for the chargeback. All Transactions charged back for a fraud-related reason that are not submitted for second presentment are considered fraudulent.

MasterCard identifies Issuers that have processed fraud-related chargebacks using message reason code 4837 (No Cardholder Authorization) or 4840 (Fraudulent Processing of Transactions) and have not reported the corresponding Transactions to SAFE. Such Transactions must otherwise be reported to SAFE within 60 days of the first chargeback date.

12.10 High Clearing Transaction Volume

MasterCard monitors Issuers with high clearing Transaction volumes that have not reported any fraudulent Transaction to SAFE during the relevant time periods. Any Issuer that has not reported fraud in a month in which the Issuer had clearing volume of at least 25,000 Transactions or in a quarter in which the Issuer had clearing volume of at least 75,000 Transactions will be identified as noncompliant with the SAFE reporting Standards.

12.11 Transaction Amount

Where appropriate, SAFE will generate a return code to identify a suspicious amount Transaction.

A suspicious amount Transaction with a return code of 24800 is a Transaction reported to SAFE that is equal to or greater than USD 9,999. A suspicious amount Transaction with a return code of 24511 is a Transaction reported to SAFE for which the Transaction amount exceeds the billing amount by more than the 25% allowable difference.

An Issuer must confirm, modify, or delete each identified suspicious amount Transaction within 60 days of receiving a return code.

12.12 Resubmitting Rejected Transactions

An Issuer must monitor Transactions rejected during submission to SAFE. The Issuer must correct and resubmit each rejected Transaction to SAFE in the following transmission. Failure to correct a rejected Transaction within 60 days of notification will result in noncompliance with SAFE reporting Standards and may result in noncompliance assessments.

12.13 Noncompliance Assessments

MasterCard, in its sole discretion, determines whether an Issuer is compliant with the SAFE reporting Standards. An Issuer that fails to timely report fraudulent Transactions to SAFE is subject to noncompliance assessments and ineligibility to claim reimbursement for incurred losses under the Excessive Chargeback Program (ECP).

After the first quarter of noncompliance, MasterCard will send an Issuer a warning letter ("First Notice") informing such Issuer that it risks being assessed for noncompliance with SAFE. The First Notice affords an Issuer the opportunity to remedy the noncompliance issue without being assessed. After two consecutive quarters of noncompliance, MasterCard will send an Issuer a noncompliance assessment letter ("Final Notice") describing any applicable assessment amounts.

12.14 Variances

MasterCard, at its sole discretion, may grant a SAFE compliance variance to an Issuer for a limited period of time due to exigent circumstances. Throughout such variance period, said Issuer must take appropriate and timely action to resolve any outstanding noncompliance issues. If an Issuer fails to become compliant by the end of the stated variance period, an assessment may be reinstated for the variance period.

NOTA: Unless noncompliance is the result of a MasterCard issue, an Issuer is required to check the Promise Agreement box, thereby agreeing to be fully SAFE compliant for a period of at least one year beginning from the end of the variance period. Any noncompliance during the Promise Period automatically puts such Issuer into Final Notice.

Capítulo 13 Global Risk Management Program

This chapter describes the Global Risk Management Program Standards and applies to all MasterCard Customers, Service Providers, and Payment Facilitators.

13.1 About the Global Risk Management Program

The MasterCard Global Risk Management Program is a tool for assessing a MasterCard Customer's current capability to manage, anticipate, and protect against internal and external risks in the issuing and acquiring portfolio.

The Global Risk Management Program also determines the effectiveness of existing fraud loss controls and other risk reduction measures and assists MasterCard Customers in identifying specific areas where such measures may be inadequate.

In addition, the Global Risk Management Program provides industry best practices to support business growth by enhancing the overall operational efficiency and profitability of the issuing and acquiring portfolio while maintaining losses at an acceptable level.

The Global Risk Management Program consists of three mandatory levels and one optional level. The three mandatory levels are Customer Onboarding Reviews for prospective MasterCard Principal Customers and MasterCard Affiliate Customers, Third Party Risk Reviews, and Customer Risk Reviews for MasterCard Principal Customers. A Maestro Customer identified by MasterCard as a Group 3 Issuer pursuant to the Maestro Issuer Loss Control Program may also be required to undergo a Customer Risk Review. A Customer may also choose to participate in Customer Consultative Reviews. This chapter describes the Standards for each review level.

13.1.1 Customer Onboarding Reviews

The Customer Onboarding Review is mandatory for any entity applying to become a MasterCard Principal Customer or a MasterCard Affiliate Customer, at the sole discretion of Global Risk Management Program staff.

The Customer Onboarding Review takes place during the initial licensing and certification stage, and requires the entity to complete one or both of the following questionnaires:

- Global Risk Management Program Issuer Questionnaire
- Global Risk Management Program Acquirer Questionnaire

If an entity that has applied to become a MasterCard Principal Customer is not in compliance with the fraud loss control Standards and the minimum requirements of fraud loss control programs described in Chapter 6, MasterCard may withhold approval of the application until the entity achieves compliance.

In addition, MasterCard reserves the right to require a Customer Risk Review if:

- Global Risk Management Program staff is dissatisfied with the response to a Customer Onboarding questionnaire (in terms of speed, content, or both), or
- Global Risk Management Program staff determines that the Customer represents a potential unacceptable risk, or potential threat to other Customers.

NOTA: There may be an additional on-site review conducted by Global Risk Management Program staff within one year of assessment of the completed questionnaire.

13.1.2 Third Party Risk Reviews

The Third Party Risk Review is an annual review conducted for selected Service Providers and Payment Facilitators, at the sole discretion of Global Risk Management Program staff.

MasterCard will examine the Service Provider's or Payment Facilitator's ability to support MasterCard Customers so that they can adhere to the minimum fraud loss control Program requirements described in Chapter 6 of this manual.

A Service Provider or Payment Facilitator that fails a Third Party Risk Review is subject to deregistration.

13.1.3 Customer Risk Reviews

MasterCard requires that each MasterCard Customer (parent and child Member ID/ICA number) conduct its issuing and acquiring Activities in a prudent and financially sound manner so as to avoid inordinate risk to itself and other Customers.

MasterCard will select MasterCard Customers for a Customer Risk Review of their systems and Programs, in an effort to determine whether the selected Customer has put in place adequate and effective fraud loss control programs and to evaluate the Customer's initial and continuing ability to avoid inordinate risk.

A MasterCard Customer must submit to and cooperate in a Customer Risk Review. MasterCard, at its sole discretion, may determine that a Customer Risk Review is necessary or appropriate.

The Customer will receive a detailed and comprehensive gap analysis report containing recommendations and benefits of critical findings during the course of the review.

If required, the report will be supplemented by an action plan.

13.1.3.1 Merchant Risk Review Requirement

A Customer selected for a Customer Risk Review that processes Transactions for e-commerce Merchants will receive the following services:

- An online survey to determine the Customer's risk level
- A scan of the Customer's Merchants' websites to determine the number of potential illegal or brand-damaging violations
- A report that includes best practices, a risk report card, and a statistical review of the Customer's number of potential illegal or brand-damaging violations

13.1.4 Customer Consultative Reviews

The Customer Consultative Review is optional and is available upon request by a Customer. This review is consultation-oriented, and is conducted on site.

The Customer will receive a detailed and comprehensive gap analysis report containing recommendations and benefits of critical findings during the course of the review.

If required, the report will be supplemented by an action plan.

13.2 Global Risk Management Program Review Topics

This section describes the topics that are covered by Global Risk Management Program reviews. Additional topics may be included at the sole discretion of MasterCard.

13.2.1 Temas de Revisión del Emisor del Programa Global de Control de Riesgos

La revisión del Emisor abordará los siguientes temas, según corresponda.

- Estructura Organizativa
- Estadísticas Operacionales
- Canales de adquisición de la tarjeta
- Agencia de venta directa
- Proceso de solicitud de tarjetas, incluyendo fraude en las solicitudes
- Puntaje de crédito
- Información de agencia de crédito
- Asignación de límite de crédito
- Manejo de Cuentas, incluyendo el manejo del límite de crédito
- Función, proceso y desempeño de autorizaciones
- Almacenamiento de datos
- Programas de control de pérdidas por fraude
- Descripción de la estrategia de implementación del Cliente en cuanto a las tecnologías de Chip/PIN de EMV, MasterCard® *SecureCode*™, y de pago sin contacto
- Políticas contra el lavado de dinero
- Desempeño y eficacia de la detección de fraude
- Estrategia de verificación de la transacción
- Investigaciones de fraude
- Análisis e identificación de Eventos de Compromiso de los Datos de la Cuenta (ADC) o de Eventos Potenciales de ADC
- Informe de fraude del Sistema para Evitar el Fraude con Eficacia (SAFE)
- Uso de MasterCard Connect™
- Política de pérdida por fraude sin cargo
- Recuperaciones y contracargos relacionados con fraude
- Recepción y uso de informes de fraude
- Pronóstico y elaboración del presupuesto de pérdida por fraude
- Metodología y análisis de sistemas de información sobre gestión

13.2.2 Temas de Revisión del Adquiriente del Programa Global de Control de Riesgos

La revisión del Adquiriente abordará los siguientes temas, según corresponda.

- Estructura Organizativa
- Estadísticas Operacionales

- Canales de adquisición del comercio (minorista y de comercio electrónico)
- Agencia de ventas directas
- Proceso de solicitud de tarjetas del comercio, incluido el fraude en las solicitudes
- Inspecciones del sitio del comercio (minorista y de comercio electrónico)
- Alerta de MasterCard para el Control de Alto Riesgo (Comercios) (MATCH™)
- Información de agencia de crédito
- Convenios de Comercio
- Capacidad de la Terminal del Punto de Venta (POS)
- Descripción de la estrategia de implementación del Cliente en cuanto a las tecnologías de Chip/PIN de EMV, MasterCard® *SecureCode*™, y de pago sin contacto
- Políticas contra el lavado de dinero
- Servicios y apoyo del comercio
- Proceso y función de las autorizaciones
- Almacenamiento de datos
- Integridad de los datos del sitio de Internet y Comercio Electrónico
- Programas de control de pérdidas por fraude y control del Comercio
- Desempeño y eficacia de la detección de fraude
- Uso de una solución de control del Comercio para evitar posibles violaciones ilegales o que perjudiquen la marca
- Estrategia de verificación de la transacción
- Investigaciones de fraude
- Análisis e identificación de Eventos de ADC o de Eventos Potenciales de ADC
- Uso de MasterCard Connect™
- Recepción y uso de informes de fraude
- Programas de acatamiento del adquiriente
- Metodología y análisis de los sistemas de información de gestión

13.3 Global Risk Management Program Reports

After a Global Risk Management Program review, the Customer or non-Customer, as the case may be, will receive a written report indicating its status as to compliance with the fraud loss control Standards and minimum fraud loss control program requirements set forth in Chapter 6, plus other required or recommended actions.

In the case of noncompliance:

- The report will indicate a number of actions that must be taken to bring the Customer or non-Customer into compliance.
- The Customer or non-Customer, as the case may be, must complete an action plan and indicate implementation dates.
- The Global Risk Management Program staff assesses the action plan and the proposed implementation dates, monitors progress and results, and determines whether the Customer's programs meet the loss control program requirements.

- The Customer may be subject to noncompliance assessments with the fraud loss control Standards set forth in Chapter 6 of this manual. Please refer to section 13.6 of this manual for more information regarding noncompliance assessments.

13.4 Customer Risk Review Conditions

The following conditions are examples of specific situations or conditions that may warrant a Customer Risk Review. Other conditions may also warrant a Customer Risk Review.

13.4.1 Customer Risk Review Issuer Criteria

MasterCard may subject an Issuer to a Customer Risk Review if any of the following conditions exist:

1. MasterCard determines that the Issuer creates or may create an unacceptable risk. By way of example and not limitation, this condition exists when:
   - The Issuer's fraud basis points or counterfeit basis points exceed two times the Regional average

     OR
   - The Issuer's fraud basis points or counterfeit basis points exceed two times the worldwide basis point average.
2. The Issuer has been identified two or more times for SAFE noncompliance.

13.4.2 Customer Risk Review Acquirer Criteria

MasterCard may subject an Acquirer to a Customer Risk Review if any of the following conditions exist:

1. MasterCard staff determines that the Acquirer creates or may create a burden to the system. By way of example and not limitation, this condition exists when:
   - The Acquirer's fraud basis points or counterfeit basis points exceed two times the Regional average (averaged over four quarters)

     OR
   - The Acquirer's fraud basis points or counterfeit basis points exceed two times the worldwide fraud basis point average (averaged over four quarters).
2. The Acquirer has six or more Merchant locations, each of which, in any one month, has:
   - Counterfeit Transactions totaling 5 percent of their total Transactions for the month, when the dollar volume associated with any counterfeit Transaction is a minimum of USD 1,000

     OR
   - At least two counterfeit Transactions in one month totaling a minimum of USD 2,500.
3. The Acquirer Counterfeit Volume Ratio (ACVR) is above a threshold ten times the worldwide ACVR.

4. The Acquirer has been notified of a violation of the Illegal or Brand-damaging Transactions Rule (Rule 5.11.7 of the *MasterCard Rules* manual).
5. The Acquirer acquires Transactions for a Merchant that has engaged in activity that MasterCard deems inappropriate in connection with use of the MasterCard brand.

13.4.3 Cálculo de los Puntos Base

El cálculo de los puntos base de fraude se realiza como sigue:

- El fraude bruto (como se reporta al SAFE) por un período de tiempo dado (tal como un trimestre o un año)
- Se divide por las ventas correspondientes (como se informaron por medio del Informe Trimestral de MasterCard [QMR]) para el mismo período de tiempo
- El resultado se multiplica por un factor de 10.000 para obtener los puntos basados en fraude.

En vista de que los puntos base de fraude se calculan usando los datos del SAFE y del QMR, se aconseja a los Clientes que coordinen con el departamento responsable de los informes al QMR para asegurar que los datos que informan sean completos, exactos y actualizados.

13.5 Global Risk Management Program Fees

The pricing principles for Global Risk Management Program reviews (questionnaires and on-site reviews) are indicated in the *MasterCard Consolidated Billing System Reports* relevant to the Customer's or non-Customer's Region.

13.6 Noncompliance with Fraud Loss Control Standards

Following a Global Risk Management Program review, a noncompliant Customer will receive a written report with requirements that must be satisfied within an established period to achieve compliance with the fraud loss control Standards and minimum fraud loss control program requirements.

If a MasterCard Customer fails to take the required actions to achieve compliance, one or more of the following may occur:

- Noncompliance assessments, as indicated in Table 13.1.
- Revocation of the Customer's License. A Customer may appeal such a revocation to MasterCard. Any decision by MasterCard is final.

Table 13.1—Noncompliance Assessments with Loss Control Program Requirements

Period	Amount assessed per month
First quarter of noncompliance	USD/EUR 25,000 per month

Period	Amount assessed per month
Second quarter of noncompliance	USD/EUR 50,000 per month
Third quarter of noncompliance	USD/EUR 75,000 per month
Each month after the third quarter of noncompliance	USD/EUR 100,000 per month

Apéndice A Contenido y Formato de los Datos de las Pistas

Este apéndice contiene información sobre los requisitos del formato de los datos de la Pista 1 y Pista 2 de la banda magnética, contenido y formato.

A.1 Track 1 Data Content and Format

Track 1 of the magnetic stripe must be encoded with the information shown in Figure A.1 and Table A.1 in the defined format, using the control character values shown in Figure A.2. The **Discretionary Data** field (the location of the CVC 1) is field 9.

NOTA: Figure A.1 represents a Track 1 data layout example in which the Account Number is 16 characters in length and the Discretionary Data is 24 characters in length.

Figure A.1—Track 1 Data Layout

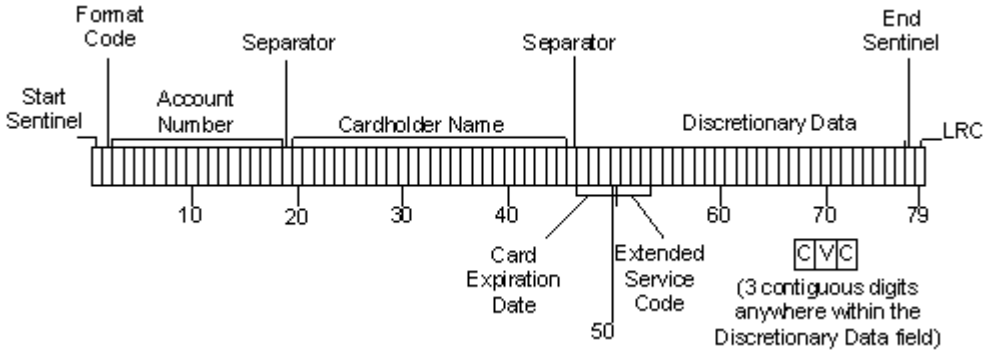

Table A.1—Track 1 Data Format and Content

Field Number	Field Name	F = Fixed Length V = Variable Length	Maximum Characters
1	Start Sentinel	F	1
2	Format Code–B (encode character B)	F	1
3	Account Number	V	19
4	Separator	F	1
5	Cardholder Name	V	2–26
6	Separator	F	1
7	Expiration Date	F	4
8	Service Code	F	3

Field Number	Field Name	F = Fixed Length V = Variable Length	Maximum Characters
9	Discretionary Data (must include CVC 1)	V	Balance of available digits not to exceed total track length of 79 characters
10	End Sentinel	F	1
11	Longitudinal Redundancy Check	F	1

Total record length—The maximum character count for Track 1 will not exceed 79 including all control characters.

Figure A.2—Track 1 Data Control Character Values

					0	0	1	1
					0	1	0	1
b4	b3	b2	b1	Row / Col	0	1	2	3
0	0	0	0	0	SP	0	@	P
0	0	0	1	1	@	1	A	Q
0	0	1	0	2	@	2	B	R
0	0	1	1	3	c	3	C	S
0	1	0	0	4	$	4	D	T
0	1	0	1	5	%d	5	E	U
0	1	1	0	6	@	6	F	V
0	1	1	1	7	@	7	G	W
1	0	0	0	8	)	8	H	X
1	0	0	1	9	(	9	I	Y
1	0	1	0	10	@	@	J	Z
1	0	1	1	11	@	@	K	b
1	1	0	0	12	@	@	L	b
1	1	0	1	13	-	@	M	b
1	1	1	0	14	.	@	N	^d
1	1	1	1	15	/	?d	O	@

Note

The positions in the table are determined by column and row; the first number being column, and the second, row. For example, 0/5 means column 0 and row 5, which is %d.

@ These characters are available for hardware control purposes only and cannot contain information characters (data content).

b These characters are reserved for additional national characters when required. They are not to be used internationally.

c This character is reserved for an optional additional graphic.

d These characters in the corresponding positions mean the following:

Position	Characters	
0/5	**% d**	represents "start sentinel"
1/15	**?d**	represents "end sentinel"
3/14	**^d**	represents "separator"

The encoded **Cardholder Name** field in Track 1 is a variable length, alphanumeric field, with a maximum length of 26 characters within (up to) three subfields. The Cardholder Name and Content Format table shown in Table A.2 defines the specifications for encoding the Cardholder name on the magnetic stripe.

Table A.2—Cardholder Name Content and Format

Element	M = Mandatory O = Optional	Length	Requirements/Comments
Surname	M	Variable	Mandatory Alphanumeric Minimum length is one character First character must be alphabetic, others may be any valid character as defined in this appendix.
Initials or First Name	O	Variable	If used, must begin with a slash (/) May be any valid characters defined in this appendix.
Title	O	Variable	If used, must begin with a period (.) Must always be after the surname and, if used, initials or first name May be any valid characters defined in this appendix.

NOTA: Characters "%", "^", and "?" cannot be used in the Cardholder Name field, because they are used only for specified encoding purposes.

The total length of the **Cardholder Name** field is 26 characters, including all control characters.

A.2 Contenido y Formato de los Datos de la Pista 2

La Pista 2 de la banda magnética deberá codificarse con la información que aparece en la Figura A.3 y en la Tabla A.3 en el formato definido, usando los valores de los caracteres de control que aparecen en la Tabla A.4. El campo **Datos Discrecionales** (la ubicación del CVC 1) es el campo 6.

NOTA: La Figura A.3 representa un ejemplo de formato de los datos de la Pista 2 en el cual el Número de Cuenta tiene 16 caracteres de longitud y los Datos Discrecionales tienen 13 caracteres de longitud.

Figura A.3—Formato de los Datos de la Pista 2

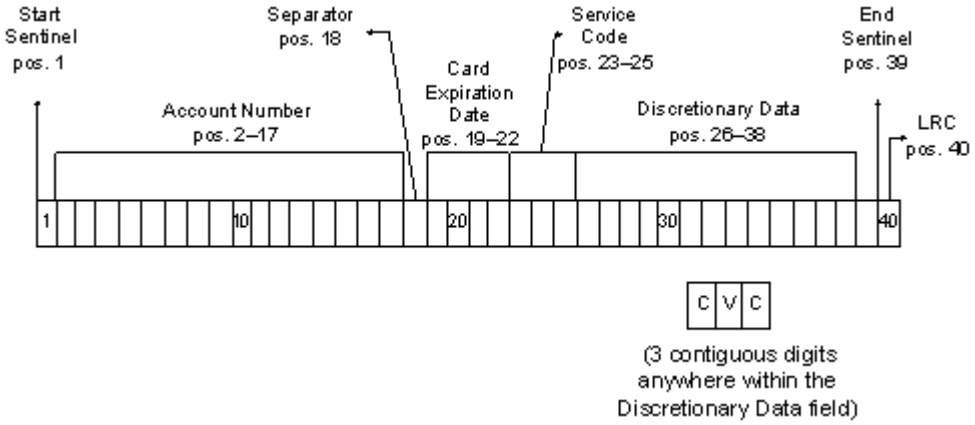

Tabla A.3—Formato y Contenido de los Datos de la Pista 2

Número del Campo	Nombre del Campo	F = Longitud Fija V = Longitud Variable	Contenido
1	Señalador de Inicio	F	Hexadecimal "B"
2	Número de Cuenta Primario (PAN)	V	Consulte las Secciones 3.2 y 3.3.
3	Separador	F	Hexadecimal "D"
4	Fecha de Vencimiento	F	Consulte la Sección 3.5.4
5	Código de Servicio	F	Consulte la Tabla 3.3 en la Sección 3.11.3.
6	Datos Discrecionales	V	
6.1	Reservado	F	La longitud es de un dígito.

Número del Campo	Nombre del Campo	F = Longitud Fija V = Longitud Variable	Contenido
6.2	Valor de Verificación del PIN (PVV)	F	La longitud es de cuatro dígitos. Se recomienda encarecidamente la codificación del PVV a fin de facilitar el uso del Emisor de los servicios on-behalf (en nombre de) de manejo de claves de PIN.
6.3	Número de Secuencia de la Tarjeta	F	La longitud es de un dígito. Identifica múltiples Tarjetas que usan el mismo PAN.
6.4	Otros Datos Discrecionales	V	Codificar el CVC 1 en tres posiciones contiguas cualesquiera después de la posición 7ª. en los datos discrecionales. El CVC 1 se requiere para las Tarjetas MasterCard y para las Tarjetas con chip de Maestro y Cirrus, emitidas recientemente o reemitidas el 11 de enero de 2013 o posteriormente con una longitud del PAN de 16 dígitos o menor.
7	Señalador de Final	F	Hexadecimal "F"
8	Verificación de Redundancia Longitudinal (LRC)	F	La longitud es de un dígito. Calcular usando la Fórmula de la LRC.

Longitud total del registro—El conteo máximo de caracteres para la Pista 2 no será mayor de 40, incluyendo todos los caracteres de control.

Los datos de la Pista 2 en la banda magnética de una Tarjeta con Chip deben ser iguales a los datos de la Pista 2 de la Aplicación de Pago correspondiente en el chip, excepto que el Emisor puede cambiar el Campo 6 (Datos Discrecionales).

Tabla A.4—Valores de los Caracteres de Control de los Datos de la Pista 2

Bits					Carácter
P	**B4**	**B3**	**B2**	**B1**	
1	0	0	0	0	0
0	0	0	0	1	1
0	0	0	1	0	2
1	0	0	1	1	3
0	0	1	0	0	4
1	0	1	0	1	5
1	0	1	1	0	6
0	0	1	1	1	7
0	1	0	0	0	8
1	1	0	0	1	9
1	1	0	1	0	(A)
0	1	0	1	1	Señalador de Inicio (Carácter de Inicio)
1	1	1	0	0	(A)
0	1	1	0	1	Separador
0	1	1	1	0	(A)
1	1	1	1	1	Señalador de Final (Carácter del Final)

Estas posiciones de caracteres (A) están disponibles únicamente para fines de control del hardware y no pueden contener caracteres de información (contenido de datos).

Apéndice B Información de Contactos

Este apéndice contiene una lista de los Contactos de MasterCard a quienes se pueden dirigir las consultas y presentar la documentación solicitada.

B.1 Servicios de Seguridad y Riesgo

Los clientes pueden enviar formularios y otra documentación relacionada con las Normas y los programas de servicio de seguridad y riesgo a:

Dirección:	América Latina Attention: Departamento de Servicios de Seguridad y Riesgo 2200 MasterCard Boulevard O'Fallon MO 63368-7263 USA
Teléfono:	1-636-722-4100 (Centro de Protección contra Fraude de MasterCard)
Teléfono:	1-914-249-5447 (Grupo de Control de Fraude de Comercios)
Fax:	1-914-249-4257
Correo electrónico:	matchhelp@mastercard.com
Correo electrónico:	mfcg@mastercard.com (Grupo de Control de Fraude de Comercios)
Télex:	0878 MSTCD UI

La correspondencia en relación a los conflictos entre las Normas y la ley aplicable debe dirigirse a la atención del Departamento Legal.

Dirección:	América Latina Attention: Law Department 2000 Purchase Street Purchase NY 10577-2509 USA

B.2 Control de Fraude del Comercio

Los clientes pueden enviar formularios y otra documentación relacionada con las Normas y los programas de control de seguridad y riesgo a:

Dirección:	América Latina Attention: Departamento de Control de Fraude del Comercio 2000 Purchase Street Purchase NY 10577-2509 USA
Teléfono:	1-914-249-5447
Fax:	1-914-249-4257
Correo electrónico:	mfcg@mastercard.com (Grupo de Control de Fraude de Comercios)

La correspondencia en relación a los conflictos entre las Normas y la ley aplicable debe dirigirse a la atención del Departamento Legal.

Dirección:	América Latina Attention: Law Department 2000 Purchase Street Purchase NY 10577-2509 USA

B.3 Eventos de Compromiso de los Datos de la Cuenta

Para obtener la información de contactos de MasterCard relacionada con los Eventos de Compromiso de los Datos de la Cuenta (ADC) o con los Eventos Potenciales de ADC, consulte la *Account Data Compromise User Guide*, disponible mediante el producto Publications [Publicaciones] de MasterCard Connect™.

B.4 Control del Diseño de Tarjetas

Los clientes pueden enviar formularios y otra documentación relacionada con el diseño y la producción de Tarjetas, tales como el Plastics Order Request Form [Formulario de Solicitud de Pedido de Plásticos] a:

Dirección:	América Latina Attention: Departamento de Control de Diseño de Tarjetas Franchise Customer Management 2000 Purchase Street Purchase NY 10577-2509 USA
Fax:	1-914-249-4499

B.5 Aplicaciones de MasterCard Connect™

Para inscribirse para una aplicación de MasterCard Connect™, visite www.mastercardconnect.com y solicite acceso a la aplicación desde el menú **MasterCard Connect Store [Tienda de MasterCard Connect]**.

Para obtener ayuda para inscribirse para una aplicación o para obtener apoyo técnico, comuníquese con Servicios de Operaciones al Cliente usando uno de los siguientes métodos:

Teléfono:	1-800-999-0363 (Región de EE. UU.)
Teléfono:	1-636-722-6636 (Fuera de la Región de EE. UU.)
Teléfono:	1-636-722-6292 (apoyo en idioma español)
Correo electrónico:	customer_support@mastercard.com

B.6 Servicios de Operaciones al Cliente

Los clientes pueden formular preguntas generales relacionadas con los programas o productos de seguridad al grupo de Servicios de Operaciones al Cliente usando uno de los siguientes métodos:

Dirección:	América Latina	
	Attention: Servicios de Operaciones al Cliente	
	2200 MasterCard Boulevard	
	O'Fallon MO 63368-7263	
	USA	
Teléfono:	1-800-999-0363 ó 1-636-722-6176 (Regiones de Canadá y EE. UU.)	
	1-636-722-6292 (apoyo en idioma español)	
	1-636-722-6176 (Todas las demás Regiones)	
Fax:	1-636-722-7192	
Correo electrónico:	Regiones de Canadá, América Latina y el Caribe, Europa, Medio Oriente/Africa y EE. UU.	customer_support@mastercard.com
	Asia/Pacífico:	
	Australia y Nueva Zelanda	csd@mastercard.com
	Brunéi/Malasia	helpdesk.malaysia@mastercard.com
	Camboya/Laos/Vietnam	helpdesk.indochina@mastercard.com
	China, Hong Kong y Taiwán	helpdesk.gc@mastercard.com
	Indonesia	helpdesk.indonesia@mastercard.com
	Japón/Guam	helpdesk.tokyo@mastercard.com
	Corea	korea_helpdesk@mastercard.com
	Filipinas	helpdesk.philippines@mastercard.com
	Singapur	helpdesk.singapore@mastercard.com
	Tailandia	helpdesk.thailand@mastercard.com
	Apoyo en idioma español	lagroup@mastercard.com
	Relaciones con Proveedores, Todas las Regiones	vendor.program@mastercard.com

B.7 Actividad Sospechosa del Comercio

Los clientes pueden enviar formularios y otra documentación relacionada con las Normas y los programas de control de fraude de la actividad Sospechosa del Comercio a:

Dirección:	América Latina Atención: QMAP—Departamento de Manejo del Fraude 2000 Purchase Street Purchase NY 10577-2509 USA
Correo electrónico:	qmap@mastercard.com

La correspondencia en relación a los conflictos entre las Normas y la ley aplicable debe dirigirse a la atención del Departamento Legal.

Dirección:	América Latina Attention: Law Department 2000 Purchase Street Purchase NY 10577-2509 USA

Apéndice C Servicios de Producción de Tarjetas

Este apéndice contiene descripciones de las actividades de producción de Tarjetas.

C.1 Servicios de Producción de Tarjetas

Las actividades en este apéndice son servicios de producción de Tarjetas. El Cliente que contrata a un proveedor para efectuar cualquiera de dichos servicios en su nombre en relación a la emisión de Tarjetas, Dispositivos de Acceso o Dispositivos de Pago Móviles debe acatar los requisitos descritos en el Capítulo 2 de este manual.

En las tablas a continuación se describen los servicios de fabricación de Tarjetas, los servicios de personalización de Tarjetas y otros servicios especializados realizados en conexión con la producción de Tarjetas.

Tabla C.1—Servicios de Fabricación de Tarjetas

Servicio	Definición
Incrustación del chip	Proceso por el cual se introduce de forma permanente un circuito integrado en una Tarjeta de pago para formar parte integral de la Tarjeta.
Fabricación de tarjetas	El proceso de producción de tarjetas está compuesto por una o más de las siguientes etapas: • Preimpresión (producción del formato del diseño de la tarjeta, películas de impresión y placas de impresión) • Impresión de las páginas plásticas blancas • Montaje de las páginas • Laminado de las páginas • Corte o perforación de las páginas • Sellado al calor del holograma y panel de la firma

Tabla C.2—Servicios de Personalización de Tarjetas

Servicio	Definición
Grabado al relieve de tarjetas	Proceso de personalización que crea caracteres realzados en el cuerpo de una Tarjeta plástica.
Codificación de tarjetas	Proceso por el cual se escriben los datos de personalización en la banda magnética localizada en la tarjeta.
Envío de tarjetas por correo	Proceso por el cual se introduce en un sobre y empaca de manera individual la Tarjeta o PIN, que se envía a una instalación de preclasificación o al servicio postal para su envío al Tarjetahabiente.

Servicio	Definición
Personalización de la tarjeta	Proceso de personalización para las Tarjetas que no están grabadas al relieve mediante el cual se escriben los datos en la Tarjeta mediante una tecnología que no es de grabado al relieve, como grabado por láser, transferencia térmica o impresión al relieve.
Personalización del chip	Proceso de "escritura" de los datos en el circuito integrado por medio de una interacción eléctrica o electromagnética entre el chip y el dispositivo de personalización. La personalización del chip generalmente ocurre después de la incrustación del chip, aunque también puede ocurrir antes o durante la incrustación del chip.

Tabla C.3—Servicios Especializados de Producción de Tarjetas

Servicio	Definición
Cumplimiento de tarjeta	Servicio independiente por el cual una Tarjeta recién emitida o re-emitida se combina con materiales adicionales obteniendo como resultado un paquete completo listo para ser distribuido al Tarjetahabiente. Una instalación aprobada para efectuar servicios de personalización también está aprobada para el cumplimiento de Tarjeta como parte de su actividad de personalización.
Preparación de datos	Servicio independiente por el cual los datos del Emisor y del Tarjetahabiente se procesan y configuran para su posterior personalización por parte del Emisor o de otro proveedor certificado. También se autoriza a una instalación aprobada para efectuar servicios de personalización para la preparación de los datos como parte de su actividad de personalización.
Recuperación por desastres	Producción de tarjetas en una instalación establecida y activada exclusivamente durante un evento de emergencia, conforme al Plan de Continuidad Empresarial (BCP) de un proveedor certificado. La producción de tarjetas en esta instalación solamente está autorizada al proveedor que la estableció. La instalación de recuperación por desastres no se debe utilizar para aliviar las restricciones de capacidad relacionadas con la producción normal de Tarjetas. Estas instalaciones se evalúan frente a un subconjunto de requisitos de seguridad y se deben actualizar para acatar el conjunto total de requisitos de seguridad al momento de la activación.
Provisión de móvil	Servicio por el que un Gerente de Servicio de Confianza (TSM) carga una aplicación de pago, proporciona los datos de personalización o envía comandos de gestión de la aplicación post-emisión a un dispositivo de pago móvil por medio de un método de comunicación inalámbrica (OTA).

Servicio	Definición
Fabricación parcial	Instalación que fabrica componentes de la Tarjeta que contienen características de seguridad o datos de personalización confidenciales, donde toda la Tarjeta es completada posteriormente por un proveedor certificado.
Impresión del PIN	Servicio independiente por el que se imprime y envía un PIN por correo. También se autoriza a un establecimiento aprobado para efectuar servicios de personalización para el envío del PIN por correo como parte de su actividad de personalización.

Apéndice D Definiciones

Los siguientes términos usados en este manual tienen el significado establecido a continuación.

Los términos adicionales y/o revisados podrán ser usados también con fines de las Reglas en un capítulo o sección específica de este manual.

Marca de Aceptación

Cualquiera de las Marcas de la Corporación que se muestra en un POI para indicar la aceptación de la marca. Consulte Marca de Aceptación de Cirrus, Marca de Aceptación de Maestro, Marca de Aceptación de MasterCard.

Dispositivo de Acceso

Un dispositivo que no sea una Tarjeta que usa al menos una Aplicación de Pago para proporcionar acceso a una Cuenta en acatamiento con las Normas. Un Dispositivo de Pago Sin Contacto es un tipo de Dispositivo de Acceso. Un Dispositivo de Acceso de Cirrus, un Dispositivo de Acceso de Maestro y un Dispositivo de Acceso de MasterCard son un Dispositivo de Acceso. *Vea también* Dispositivo de Pago Móvil.

Cuenta

Una cuenta mantenida por o en nombre de un Tarjetahabiente por un Emisor para el procesamiento de Transacciones, y que se identifica con un número de identificación bancaria (BIN) o número de identificación del emisor (IIN) designado por la Corporación en sus tablas de distribución para la distribución al Sistema de Intercambio. *Vea también* Cuenta de Cirrus, Cuenta de Maestro, Cuenta de MasterCard.

Sistema de Activación de Cuentas

Efectúa los servicios de activación de la Cuenta para los Pagos de MasterCard Basados en la Nube, que pueden incluir las verificaciones de elegibilidad del Dispositivo de Acceso y de la Cuenta, la Identificación y Verificación (ID&V), la Digitalización y el manejo posterior del ciclo de duración.

PAN de la Cuenta

Número de cuenta primario (PAN) asignado a una cuenta por un emisor.

Rango de PAN de la Cuenta

Rango de los PAN de la Cuenta designado por un Emisor para su Digitalización.

Adquiriente

Un Cliente en su capacidad de adquiriente de una Transacción.

Activity(ies)

The undertaking of any act that can be lawfully undertaken only pursuant to a License granted by the Corporation. *Also see* Digital Activity(ies).

Cliente Afiliado, Afiliado

Un Cliente que participa indirectamente en la Actividad a través del Patrocinio de un Principal o exclusivamente con respecto a la Actividad de MasterCard a través del Patrocinio de una Asociación. Un Afiliado no puede Patrocinar a ningún otro Cliente.

Area de Uso

El país o los países en los que el Cliente tiene Licencia para usar las Marcas y realizar la Actividad y que, por lo general, está establecido en la Licencia o en un anexo de la Licencia.

Cliente de Asociación, Asociación

Un Cliente de MasterCard que participa directamente en la Actividad de MasterCard por medio del uso de sus BIN asignados y que puede Patrocinar uno o más Afiliados de MasterCard pero no puede emitir directamente las Tarjetas MasterCard o adquirir Transacciones de MasterCard sin el explícito consentimiento previo por escrito de la Corporación.

Cargo por Acceso a ATM

Un cargo que cobra un Adquiriente en relación a un retiro de efectivo o Depósito Compartido iniciado en la Terminal de ATM del Adquiriente con una Tarjeta, y agregado al monto total de la Transacción transmitido al Emisor.

Convenio de Propietario de ATM

Convenio entre un propietario de ATM y un Cliente en el que se establecen los términos en virtud de los cuales el ATM acepta las Tarjetas.

Terminal de ATM

Cualquier ATM que permita a un Tarjetahabiente efectuar una Transacción con una Tarjeta conforme a las Normas.

Transacción de ATM

Un retiro de efectivo efectuado en una Terminal de ATM con una Tarjeta y procesado por medio de la Red de ATM de MasterCard. Una Transacción de ATM se identifica con el MCC 6011 (Desembolsos de Efectivo Automatizados—Institución Financiera Cliente).

Cajero Automático (ATM)

Dispositivo de autoservicio sin atención de personal que realiza funciones bancarias básicas, tales como aceptación de depósitos, retiros de efectivo, solicitudes de transferencia entre cuentas, pagos de préstamos y consultas de saldo de la cuenta.

BIN

A bank identification number (BIN, sometimes referred to as an issuer identification number, or IIN) is a unique number assigned by MasterCard for use by a Customer in accordance with the Standards.

Cargo de la Marca

Un cargo que se cobra por ciertas Transacciones no distribuidas al Sistema de Intercambio.

Marca Principal

Una Palabra Registrada en forma de leyenda de letras personalizadas colocada dentro del diseño de círculos entrelazados de la Corporación. La Marca de MasterCard, la Marca de Maestro y la Marca de Cirrus constituyen una Marca Principal.

Tarjeta

Tarjeta emitida por un Cliente conforme a la Licencia y de acuerdo con las Normas y que proporciona acceso a una Cuenta. A menos que en este documento se disponga lo contrario, las Normas aplicables al uso y aceptación de una Tarjeta también son aplicables a un

Dispositivo de Acceso y, en un entorno Sin tarjeta presente, una Cuenta. Una Tarjeta Cirrus, Tarjeta Maestro, Tarjeta MasterCard constituyen una Tarjeta.

Tarjetahabiente

Usuario autorizado de una Tarjeta o Dispositivo de Acceso emitido por un Cliente.

Comunicación al Tarjetahabiente

Cualquier comunicación del Emisor o en nombre de un Emisor a un Tarjetahabiente o posible Tarjetahabiente. Una Solicitación es un tipo de Comunicación al Tarjetahabiente.

Método de Verificación del Tarjetahabiente (CVM)

Proceso utilizado para confirmar que la persona que presenta la Tarjeta es el un Tarjetahabiente autorizado. La Corporación considera los siguientes CVM como válidos cuando se usan conforme a las Normas:

- La comparación, por parte del Comercio o Adquiriente que acepta la Tarjeta, de la firma en el panel de la firma de la Tarjeta con la firma proporcionada en el recibo de la Transacción por parte de la persona que presenta la Tarjeta;
- La comparación, por parte del Emisor de la Tarjeta o del chip de EMV en la Tarjeta, del valor ingresado en un teclado para marcar el PIN de la Terminal con el número de identificación personal (PIN) otorgado a, o seleccionado por, el Tarjetahabiente tras la emisión de la Tarjeta; y
- El uso de un CVM del Dispositivo del Consumidor (CDCVM) que MasterCard aprobó como CVM válido para las Transacciones después de completar correctamente los procedimientos de certificación y pruebas estipulados en la sección 3.9 del manual *Security Rules and Procedures*.

En determinados entornos con Tarjeta presente, un Comercio puede completar la Transacción sin un CVM ("sin CVM" como el CVM), tal como en las Transacciones del Servicio de Pago Rápido (QPS), Transacciones Sin Contacto menores o iguales al límite del CVM, y en las Transacciones en Terminales de POS sin atención de personal, identificadas como Terminales activadas por el Tarjetahabiente (CAT) de Nivel 2 o de Nivel 3.

Tarjeta con Chip (Tarjeta Inteligente, Tarjeta de Circuito Integrado, Tarjeta de IC o ICC)

Una Tarjeta con un chip incrustado que acata las normas de EMV y que contiene capacidades interactivas y de memoria utilizadas para identificar y almacenar datos adicionales acerca de un Tarjetahabiente, una Cuenta, o ambos.

Terminal MPOS con capacidad de Chip solamente

Una Terminal MPOS que contiene un lector de chip de contacto y que no posee capacidad de lectura por medio de banda magnética y que debe:

1. Funcionar como una Terminal del POS en línea solamente con fines de autorización;
2. Apoyar la firma o No CVM Requerido como método de verificación del Tarjetahabiente, y que también puede apoyar la verificación del PIN si se realiza por medio de un dispositivo de ingreso del PIN (PED) que cumple con el Programa de Evaluación y Requisitos de Seguridad del PED del POS de la Industria de Tarjetas de Pago (PCI); y
3. Que, por lo demás, cumple con los requisitos de la Corporación para las Terminales del POS Híbridas.

Transacción con Chip

Una Transacción con Chip Con Contacto o una Transacción con Chip Sin Contacto

Marca de Aceptación Cirrus

Una Marca que consiste en la Marca Principal Cirrus colocada en el rectángulo de aceptación azul oscuro disponible en www.mastercardbrandcenter.com.

Dispositivo de Acceso de Cirrus

Un Dispositivo de Acceso que utiliza al menos una Aplicación de Pago de Cirrus para proporcionar acceso a una Cuenta de Cirrus cuando se usa en una Terminal de ATM o en una Terminal En Sucursales basada en PIN.

Cuenta de Cirrus

Una cuenta elegible para ser una Cuenta de Cirrus, como se estipula en la Regla 6.1.3.2 del manual *Reglamento de MasterCard*, e identificada con un BIN/IIN relacionado con una cartera designada por la Corporación como una Cartera de Cirrus en sus tablas de distribución.

Marca Cirrus

Una Marca que consiste en la Palabra Registrada de Cirrus en forma de leyenda de letras personalizadas colocada dentro del diseño de círculos entrelazados de la Corporación. La Corporación es la propietaria exclusiva de la Marca Cirrus.

Tarjeta Cirrus

Tarjeta que proporciona acceso a una Cuenta de Cirrus.

Cliente de Cirrus

Un Cliente al que se le ha otorgado una Licencia de Cirrus conforme con las Normas.

Cirrus Payment Application

A Payment Application that stores Cirrus Account data.

Palabra Registrada de Cirrus

Una Marca que consiste en la palabra "Cirrus" seguida de una marca comercial registrada ® o ™ símbolo (según el estado de su marca comercial en un país particular) o el equivalente de la ley local. "Cirrus" debe aparecer en inglés y se debe escribir correctamente, con la letra "C" en mayúscula. "Cirrus" no se debe abreviar, separar con guion, usar en plural o en posesivo, ni traducir a otro idioma. La Corporación es la propietaria exclusiva de la Palabra Registrada de Cirrus.

Red de ATM de la Competencia

Una Red de ATM Internacional de la Competencia o una Red de ATM Norteamericana de la Competencia, según sea el caso.

Red del POS de EFT de la Competencia

Una red, diferente a cualquier red de propiedad y operada por la Corporación, que proporciona acceso a las Cuentas de Maestro en las Terminales del POS mediante el uso de tarjetas de pago y tiene las siguientes características:

1. Proporciona una marca o marcas de servicio común para identificar la Terminal del POS y las tarjetas de pago, que proporcionan el acceso a la Cuenta de Maestro;
2. No es un afiliado a la Corporación; y
3. Opera en al menos un país en el que la Corporación ha otorgado una Licencia o Licencias.

Las siguientes redes están diseñadas, sin límites, para ser Redes del POS de EFT de la Competencia: Interlink; Electron; y V-Pay.

Red Internacional de ATM de la Competencia

Una red de ATM y de tarjetas de pago, que no son de la Corporación, identificadas con una marca común que se usa exclusivamente o, principalmente, para el intercambio de ATM que:

1. Funciona en al menos tres países;
2. Usa una marca o marcas de servicio común para identificar los ATM y las tarjetas de pago, que proporcionan el acceso a la cuenta a través de ellos; y
3. Proporciona acceso a la cuenta a por lo menos 40.000.000 tarjetas de débito por medio de al menos 25.000 ATM.

Red de ATM de Norteamérica de la Competencia

Una red de ATM y de tarjetas de pago, que no son de la Corporación, identificadas con una marca común que se usa exclusivamente o, principalmente, para el intercambio de ATM y que posee todas las siguientes características:

1. Opera por lo menos en 40 de los estados o provincias de los estados y provincias de Estados Unidos y Canadá;
2. Usa una marca o marcas de servicio común para identificar las terminales y las tarjetas que proporcionan el acceso a la cuenta a través de la red;
3. Existen por lo menos 40,000,000 tarjetas de débito que proporcionan acceso a las cuentas a través de la red; y
4. Existen por lo menos 12,000 ATMs que proporcionan acceso a las cuentas a través de la red.

Método de Verificación del Tarjetahabiente del Dispositivo del Consumidor, CVM del Dispositivo del Consumidor, CDCVM

Un CVM que ocurre cuando se ingresan las credenciales personales establecidas por el Tarjetahabiente para obtener acceso a una Cuenta por medio de un Dispositivo de Acceso particular en el Dispositivo de Acceso y se verifican, ya sea dentro del Dispositivo de Acceso o mediante el Emisor durante la autorización en línea. Un CDCVM es válido si el Emisor ha aprobado el uso del CVM para la autenticación del Tarjetahabiente.

Transacción con Chip de Contacto

Una Transacción en la que se intercambian datos entre la Tarjeta con Chip y la Terminal mediante la lectura del chip utilizando una interfaz de contacto, en conformidad con las especificaciones de EMV.

Dispositivo de Pago Sin Contacto

Un medio diferente a una Tarjeta por el cual un Tarjetahabiente puede acceder a una Cuenta en una Terminal de acuerdo con las Normas. Un Dispositivo de Pago Sin Contacto es un tipo de Dispositivo de Acceso que intercambia datos con la Terminal por medio de las comunicaciones de radio frecuencia. *Vea también* Dispositivo de Pago Móvil.

Contactless Transaction

A Transaction in which data is exchanged between the Chip Card or Access Device and the Terminal through the reading of the chip using the contactless interface, by means of radio frequency communications. *Also see* EMV Mode Contactless Transaction, Magnetic Stripe Mode Contactless Transaction.

Control, Controlado

A efectos de este documento, Control tiene el significado que la Corporación considere adecuado a su exclusiva discreción según el contexto de uso del término y todos los factores y circunstancias que la Corporación considere adecuados tener en cuenta. En general, Control a menudo significa tener, solo o junto con otra entidad o entidades, la posesión directa, indirecta, legal o productiva (por contrato o de otro modo) del poder de dirigir la administración o las políticas de otra entidad.

Corporación

MasterCard International Incorporated, Maestro International Inc., y sus subsidiarias y afiliados. A efectos de este documento, Corporación también significa el Presidente y el Presidente Ejecutivo Principal de MasterCard International Incorporated, o su designado, u otros funcionarios o empleados responsables de la administración y/o manejo de un programa, servicio, producto, sistema u otra función. A menos que se especifique de otro modo en las Normas, y sujeto a cualquier restricción impuesta por la ley o las regulaciones o por la Junta Directiva de MasterCard International Incorporated, o por o el Acta de Constitución de MasterCard International Incorporated o por el Acta de Constitución de MasterCard Incorporated (según dicha Acta de Constitución pueda enmendarse en un momento dado), cada una de dichas personas tiene la autorización de actuar en nombre de la Corporación y de actuar a su entera discreción.

Credentials Management System

Facilitates credential preparation and/or remote mobile Payment Application management for MasterCard Cloud-Based Payments.

Transacción Transfronteriza

Transacción que se origina en un establecimiento que acepta la Tarjeta, en un país diferente del país en el cual se emitió la Tarjeta.

Customer

A financial institution or other entity that has been approved for Participation. A Customer may be a Principal, Association, Affiliate, or Digital Activity Customer. *Also see* Cirrus Customer, Maestro Customer, MasterCard Customer, Member.

Informe del Cliente

Cualquier informe que el Cliente debe proporcionar a la Corporación, tanto si es una sola vez como varias veces, relacionado con su Licencia, sus Actividades, el uso de cualquier Marca o cualquier asunto de ese tipo. A modo ilustrativo y no limitativo, el Informe Trimestral de MasterCard (QMR) es un Informe del Cliente.

Entidad de Almacenamiento de Datos (DSE)

Un Proveedor de Servicios que efectúa uno o más de los servicios descritos en la Regla 7.1 del manual *Reglamento de MasterCard* como un Servicio del Programa DSE.

Device Binding

The process by which a Wallet Token Requestor binds a MasterCard Token corresponding to a Cardholder's Account to that Cardholder's Mobile Payment Device, which may consist of:

- The provisioning of the Token and its associated encryption keys into the secure element within the Mobile Payment Device;
- The loading of an application for a remotely-managed secure server into the Mobile Payment Device and the successful communication of the device with the application; or
- Other methodology acceptable to the Corporation.

Actividades Digitales

La realización de cualquier acto que pueda ser realizado legalmente, solamente conforme a la aprobación por parte de la Corporación, según se establece en un Convenio de Actividad Digital o en otra documentación escrita. La participación en el Servicio de Activación Digital de MasterCard como un Solicitante de Token de Billetera es una Actividad Digital.

Digital Activity Agreement

The contract between the Corporation and a Digital Activity Customer granting the Digital Activity Customer the right to participate in Digital Activity and a limited License to use one or more of the Marks in connection with such Digital Activity, in accordance with the Standards.

Cliente de Actividad Digital

Cliente que participa en Actividad Digital conforme a un Convenio de Actividad Digital y que no podrá emitir Tarjetas, adquirir Transacciones ni Patrocinar ningún otro Cliente a la Corporación.

Digital Activity Service Provider (DASP)

A Service Provider that performs any one or more of the services described in Rule 7.1 of the *MasterCard Rules* as DASP Program Service.

Digital Goods

Any goods that are stored, delivered, and used in electronic format, such as, by way of example but not limitation, books, newspapers, magazines, music, games, game pieces, and software (excludes gift cards). The delivery of a purchase of digital goods may occur on a one-time or subscription basis.

Digital Wallet

A Pass-through Digital Wallet or a Staged Digital Wallet.

Operador de Billetera Digital (DWO)

Un Proveedor de Servicios que efectúa uno o más de los servicios descritos en la Regla 7.1 del manual *Reglamento de MasterCard* como un Servicio del Programa DWO. *Consulte también* Operador de Billetera Digital por Etapas y Operador de Billetera Digital de Transferencia.

Marca de Operador de Billetera Digital, Marca de DWO

Una marca que identifica una Billetera Digital de Transferencia y/o una Billetera Digital por Etapas particular, y que se puede exhibir en el POI para indicar que un minorista, o cualquier otra persona, empresa o corporación acepta pagos efectuados por medio de esa Billetera

Digital de Transferencia y/o Billetera Digital por Etapas. Tanto una "Marca de DWO por Etapas" como una "Marca de DWO de Transferencia" son Marcas de DWO.

Digitalización, Digitar

Preparación de los datos efectuada en nombre del Emisor antes de la provisión de las credenciales de la Cuenta, en la forma de un Token de MasterCard, en un Dispositivo de Pago Móvil conectado o en un servidor de Simulación de Tarjeta de la Computadora Principal (HCE) después de la Identificación y Verificación (ID&V). La digitalización incluye la Tokenización.

Transacción Nacional

Vea Transacción Nacional.

Dual Interface

The description of a Terminal that is capable of processing Contactless Transactions by means of its contactless interface and Contact Chip Transactions by means of its contact interface.

Dinero Electrónico

Valor monetario al que se accede de manera electrónica (incluyendo magnéticamente) como se representa mediante una reclamación al Emisor de Dinero Electrónico que:

1. Es emitido al recibir fondos con el fin de hacer transacciones con tarjetas de pago; y
2. Es aceptado por el Emisor de Dinero Electrónico o una persona diferente al Emisor de Dinero Electrónico.

Institución de Dinero Electrónico

Una entidad autorizada por la autoridad reguladora correspondiente u otra entidad gubernamental como una "institución de dinero electrónico", "institución de dinero-e", "pequeña institución de dinero electrónico" o cualquier otra calificación aplicable bajo la cual la entidad está autorizada a emitir o adquirir transacciones de Dinero Electrónico bajo la ley o normativa correspondiente.

Emisor de Dinero Electrónico

Una Institución de Dinero Electrónico con respecto a sus actividades de emisión solamente.

Transacción Sin Contacto en Modo EMV

Una Transacción Sin Contacto en la que la Terminal y el chip intercambian datos, permitiendo que el chip apruebe la Transacción fuera de línea en nombre del Emisor o solicite autorización en línea del Emisor, en acatamiento con las Normas.

Cliente del Gateway

Un Cliente que usa el servicio de Procesamiento del Gateway.

Procesamiento del Gateway

Un servicio que permite que un Cliente envíe una Transacción del Gateway y/o reciba una Transacción del Gateway de la Red de ATM de MasterCard®.

Transacción del Gateway

Una transacción de ATM efectuada con una tarjeta de pago u otro dispositivo de acceso que no lleva Marca que se procesa a través o por medio del uso de la Red de ATM de MasterCard®.

Simulación de Tarjeta de la Computadora Principal (HCE)

Presentación en un Dispositivo de Pago Móvil de una representación virtual y exacta de una Tarjeta con Chip usando solamente software en el Dispositivo de Pago Móvil y que se lleva a cabo por medio de su comunicación con un servidor seguro a distancia.

Hybrid Terminal

A Terminal, including any POS or MPOS Terminal ("Hybrid POS Terminal", "Hybrid MPOS Terminal"), ATM Terminal ("Hybrid ATM Terminal"), or PIN-based In-Branch Terminal ("Hybrid PIN-based In-Branch Terminal"), that:

1. Is capable of processing both Contact Chip Transactions and magnetic stripe Transactions;
2. Has the equivalent hardware, software, and configuration as a Terminal with full EMV Level 1 and Level 2 type approval status with regard to the chip technical specifications; and
3. Has satisfactorily completed the Corporation's Terminal Integration Process (TIP) in the appropriate environment of use.

Identification & Verification (ID&V)

The identification and verification of a person as the Cardholder to whom the Issuer allocated the Account PAN to be Tokenized.

Organización Independiente de Ventas (ISO)

Un Proveedor de Servicios que efectúa uno o más de los servicios descritos en la Regla 7.1 del manual *Reglamento de MasterCard* como un Servicio del Programa de la ISO.

Sistema de Intercambio

El conjunto de hardware y software de computación que opera la Corporación o que se opera en su nombre para la distribución, procesamiento y liquidación de las Transacciones, incluyendo, entre otras cosas, la Red de MasterCard, la Red de ATM de MasterCard, el Sistema de Mensaje Dual, el Sistema de Mensaje Individual, el Sistema de Manejo de Compensación Global (GCMS) y el sistema de Manejo de Cuentas de Liquidación (SAM).

Transacciones Entre Países de Europa

Una Transacción completada por medio de una Tarjeta emitida en un país o territorio que se indica en la Zona Unica de Pagos en Euros (SEPA) en una Terminal ubicada en un país o territorio indicado en la Zona No Unica de Pagos en Euros (No de SEPA) o una Transacción completada usando una Tarjeta emitida en un país o territorio que se indica en la Zona de Pagos en Euros No Unica (No de SEPA) en una Terminal ubicada en un país o territorio que se indica en la Zona Unica de Pagos en Euros (SEPA).

Transacción Entre Regiones

Transacción que se origina en un establecimiento que acepta la Tarjeta, en una Región diferente de la Región en la cual se emitió la Tarjeta. En la Región de Europa, el término «Transacción Entre Regiones» incluye las «Transacciones Entre Países de Europa», como se define dicho término en el capítulo «Región de Europa» del *Reglamento de MasterCard*.

Transacción Nacional

Transacción que se origina en un establecimiento que acepta la Tarjeta, en el mismo país que el país en el cual se emitió la Tarjeta. Una Transacción efectuada con una Tarjeta que lleva una o más de las Marcas Principales, ya sea sola o combinada con las marcas de otro esquema de pago y procesada como una Transacción, como muestra la identificación del tipo de Tarjeta en

el registro de la Transacción, por medio del Sistema de Intercambio o de una red diferente, califica como una Transacción Nacional. "Transacción Local" es un término alternativo para Transacción Nacional.

Transacciones Dentro de Europa

Una Transacción Dentro de la Zona que No es SEPA o una Transacción Dentro de la Zona de SEPA, pero no una Transacción Entre Países de Europa.

Transacciones Dentro de una zona que No es SEPA

Una Transacción completada por medio de una Tarjeta emitida en un país o territorio que se indica en la Zona No Unica de Pagos en Euros (No de SEPA) en una Terminal ubicada en un país o territorio indicado en la Zona No Unica de Pagos en Euros (No de SEPA).

Transacción Dentro de la Región

Transacción que se origina en un establecimiento que acepta la Tarjeta, en un país diferente del país en el cual se emitió la Tarjeta, dentro de la misma Región. En la Región de Europa, este término se reemplaza por «Transacción Dentro de Europa», como se define dicho término en el capítulo «Región de Europa» del *Reglamento de MasterCard*.

Emisor

Un Cliente en su capacidad como emisor de una Tarjeta o Cuenta.

Licencia, con Licencia

Contrato entre la Corporación y un Cliente en el cual se otorga al Cliente el derecho de usar una o más de las Marcas de acuerdo con las Normas. Tener "Licencia" significa tener dicho derecho de acuerdo con una Licencia.

Licenciatario

Un Cliente u otra persona autorizada por escrito por la Corporación a usar una o más de las Marcas.

Maestro

Maestro International Incorporated, una corporación de Delaware EE. UU. o cualquier sucesor de ello.

Marca de Aceptación de Maestro

Una Marca que consiste en la Marca Principal Maestro colocada en el rectángulo de aceptación azul oscuro disponible en www.mastercardbrandcenter.com.

Dispositivo de Acceso de Maestro

Un Dispositivo de Acceso que utiliza al menos una Aplicación de Pago de Maestro para proporcionar acceso a una Cuenta de Maestro cuando se usa en una Terminal.

Cuenta de Maestro

Una cuenta elegible para ser una Cuenta de Maestro, como se estipula en la Regla 6.1.2.1 del manual *Reglamento de MasterCard*, e identificada con un BIN/IIN relacionado con una Cartera designada por la Corporación como una Cartera de Maestro en sus tablas de distribución.

Marca de Maestro

Una Marca que consiste en la Palabra Registrada de Maestro en forma de leyenda de letras personalizadas colocada dentro del diseño de círculos entrelazados de la Corporación. La Corporación es la propietaria exclusiva de la Marca Maestro.

Tarjeta Maestro

Tarjeta que proporciona acceso a una Cuenta de Maestro.

Cliente de Maestro

Un Cliente al que se le ha otorgado una Licencia de Maestro conforme con las Normas.

Maestro Payment Application

A Payment Application that stores Maestro Account data.

Palabra Registrada de Maestro

Una Marca que consiste de la palabra "Maestro" seguida de una marca comercial registrada ® o ™ símbolo (según el estado de su marca comercial en un país particular) o el equivalente de la ley local. "Maestro" debe aparecer en inglés y se debe escribir correctamente, con la letra "M" en mayúscula. "Maestro" no se debe abreviar, separar con guion, usar en plural o en posesivo, ni traducir a otro idioma. Maestro es el propietario exclusivo de la Marca Principal Maestro.

Transacción Sin Contacto en Modo de Banda Magnética

Es una Transacción Sin Contacto en la que la Terminal recibe los datos estáticos y dinámicos desde el chip y construye mensajes que se pueden transportar en un formato de mensaje de banda magnética estándar, en acatamiento con las Normas.

Transacción de Desembolso de Efectivo Manual

Un desembolso de efectivo efectuado después de la aceptación de una Tarjeta MasterCard o, en una Terminal En Sucursales basada en PIN, una Tarjeta Maestro o Cirrus por parte del cajero de una institución financiera Cliente. Una Transacción de Desembolso de Efectivo Manual se identifica con el MCC 6010 (Desembolso de Efectivo Manual—Institución Financiera Cliente).

Marcas

Los nombres, logos, nombres comerciales, logotipos, marcas comerciales, marcas de servicio, designaciones comerciales y otras designaciones, símbolos y marcas que la Corporación posee, administra, concede licencias o, de otra manera, Controla y pone a disposición para el uso de los Clientes y de otras entidades autorizadas conforme a una Licencia. Una "Marca" significa cualquiera de las Marcas.

MasterCard

MasterCard International Incorporated, una corporación de Delaware EE. UU.

Marca de Aceptación MasterCard

Una Marca que consiste en la Marca Principal MasterCard colocada en el rectángulo de aceptación azul oscuro disponible en www.mastercardbrandcenter.com.

Dispositivo de Acceso de MasterCard

Un Dispositivo de Acceso que utiliza al menos una Aplicación de Pago de MasterCard para proporcionar acceso a una Cuenta de MasterCard cuando se usa en una Terminal.

Cuenta de MasterCard

Cualquier tipo de cuenta (crédito, débito, prepagada, comercial, etc.) identificada como una Cuenta de MasterCard con un número de cuenta primario (PAN) que comienza con un BIN en el rango de 222100 a 272099 ó 510000 a 559999.

Identificador de la Aplicación de la marca MasterCard (AID)

Cualquiera de los identificadores de la aplicación de chip de EMV de la Corporación para las Aplicaciones de Pago de MasterCard, Maestro y Cirrus según se define en el manual *M/Chip Requirements*.

Marca de MasterCard

Una Marca que consiste en la Palabra Registrada MasterCard en forma de leyenda de letras personalizadas colocada dentro del Diseño de Círculos Entrelazados de MasterCard. La Corporación es la propietaria exclusiva de la Marca de MasterCard.

Tarjeta MasterCard

Tarjeta que proporciona acceso a una Cuenta de MasterCard.

MasterCard Cloud-Based Payments

A specification that facilitates the provisioning of Digitized Account data into a Host Card Emulation (HCE) server and the use of the remotely stored Digitized Account data, along with single-use payment credentials, in Transactions effected by a Cardholder using a Mobile Payment Device. The MasterCard Digital Enablement Service offers MasterCard Cloud-Based Payments as an on-behalf service.

Cliente de MasterCard

Un Cliente al que se le ha otorgado una Licencia de MasterCard conforme con las Normas. *Vea también* Miembro.

MasterCard Digital Enablement Service

Any of the services offered by the Corporation exclusively to Customers for the digital enablement of Account data, including but not limited to ID&V Service, Tokenization Service, Digitization Service, Token Mapping Service, MasterCard Cloud-Based Payments, Digital Card Image Database, CVC 3 pre-validation and other on-behalf cryptographic validation services, and Service Requests.

MasterCard Europe

MasterCard Europe SA, una compañía de responsabilidad limitada de Bélgica (compañía).

MasterCard Incorporated

MasterCard Incorporated, una corporación de Delaware EE. UU.

MasterCard Payment Application

A Payment Application that stores MasterCard Account data.

Token de MasterCard

Token asignado de un Rango de Cuentas de Token de MasterCard que la Corporación ha designado a un Emisor y que corresponde a un PAN de la Cuenta para el cual el Tarjetahabiente del Emisor ha solicitado la Digitalización. La Corporación es propietaria exclusiva de todos los derechos, títulos e intereses en cualquier Token de MasterCard.

Rango de Cuentas de Token de MasterCard

Número de Identificación Bancaria (BIN) o parte de un BIN ("rango de BIN") designado por la Corporación a un Emisor para la asignación de Token de MasterCard en una Implementación de Token específica. Un Rango de Cuentas de Token de MasterCard debe designarse de un BIN reservado para la Corporación por la Autoridad de Registros de la ISO y para el cual la

Corporación es, por lo tanto, el "Controlador de BIN", según define dicho término en la Estructura de Trabajo Técnica de las Especificaciones de la Tokenización de Pago de EMV (consulte también el término "Rango de BIN de Token" en ese documento). Un Rango de Cuentas de Token de MasterCard se identifica en las tablas de distribución de la Corporación como que tiene los mismos atributos que el Rango de PAN de la Cuenta correspondiente.

Caja Fuerte de Token de MasterCard

Caja Fuerte de Token propiedad de MasterCard, operada por la misma y habilitada por medio del Servicio de Activación Digital de MasterCard.

Palabra Registrada MasterCard

Una Marca que consiste en la palabra "MasterCard", seguida de un símbolo de marca registrada® o el equivalente en la legislación local. "MasterCard" debe aparecer en inglés y se debe escribir correctamente, con las letras "M" y "C" en mayúscula. "MasterCard" no se debe abreviar, separar con guión, usar en plural o en posesivo, ni traducir a otro idioma. La Corporación es la propietaria exclusiva de la Palabra Registrada MasterCard.

Miembro, Membresía

Una institución financiera u otra entidad aprobada para ser un Cliente de MasterCard de acuerdo con las Normas y que, como Cliente de MasterCard, se le ha concedido la membresía ("Membresía") y se ha convertido el miembro ("Miembro") de la Corporación. "Membresía" significa también "Participación".

Transacción de Mercancías

La compra efectuada por parte de un Tarjetahabiente de mercancías o un servicio, pero no de moneda, en una categoría aprobada en una Terminal de ATM y dispensada o proporcionada, de otra manera, por dicha Terminal de ATM. Una Transacción de Mercancías se identifica con el MCC 6012 (Mercancía y Servicios—Institución Financiera Cliente), a menos que se especifique de otra manera.

Comercio

Vendedor al por menor o cualquier otra persona, firma o corporación que, de acuerdo con un Convenio Comercial, conviene en aceptar Tarjetas cuando se presenten adecuadamente.

Convenio de Comercio

Un convenio entre un Comercio y un Cliente en el que se establecen los términos en virtud de los cuales se autoriza al Comercio a aceptar Tarjetas.

Dispositivo de Pago Móvil

Un teléfono móvil controlado por el Tarjetahabiente que contiene una Aplicación de Pago que acata las Normas, y que utiliza una pantalla y un teclado integrado para acceder a una Cuenta. Un Dispositivo de Pago Móvil es un tipo de Dispositivo de Pago Sin Contacto.

Terminal de POS Móvil (MPOS)

Una Terminal MPOS permite usar un dispositivo móvil como una Terminal de POS. La funcionalidad de software y "lectura" de la tarjeta que cumple con los requisitos de la Corporación puede residir en el dispositivo móvil, en un servidor al cual se accede por medio del dispositivo móvil o en un accesorio separado conectado (mediante Bluetooth o un puerto USB) al dispositivo móvil. El dispositivo móvil puede ser cualquier plataforma de computación móvil con múltiples fines, incluyendo, a modo ilustrativo y no limitativo, un teléfono, un teléfono inteligente, una tableta o un asistente digital personal (PDA).

Multi-Account Chip Card

A Chip Card with more than one Account encoded in the chip.

Verificación del Tarjetahabiente en el Dispositivo

El uso de un CDCVM como CVM para una Transacción.

Propiedad, Propietario

A efectos de este documento, Propiedad tiene el significado que la Corporación considere adecuado a su exclusiva discreción según el contexto de uso del término en todos los factores y circunstancias que la Corporación considere adecuado tener en cuenta. En general, propiedad a menudo significa la posesión indirecta, legal o productiva de más del cincuenta por ciento (50%) de una entidad.

Participation

The right to participate in Activity, Digital Activity, or both granted to a Customer by the Corporation. For a MasterCard Customer, Participation is an alternative term for Membership.

Billetera Digital de Transferencia

Funcionalidad a través de la cual el Operador de Billetera Digital de Transferencia almacena los datos de la Cuenta de MasterCard o Maestro proporcionados por el Tarjetahabiente al DWO con el fin de efectuar un pago iniciado por el Tarjetahabiente a un Comercio o Comercio Secundario, y después de efectuada una Transacción, transfiere los datos de la Cuenta al Comercio o Comercio Secundario o a su Adquiriente o al Proveedor de Servicios del Adquiriente.

Operador de Billetera Digital (DWO) de Transferencia

El operador de una Billetera Digital de Transferencia.

Aplicación de Pago

La funcionalidad de banda magnética o de M/chip que almacena los datos de una Cuenta en una Tarjeta o Dispositivo de Acceso y que permite la lectura mediante y/o transmisión de dichos datos a una Terminal mediante una interfaz, con o sin contacto, o Pago a Distancia Digital Garantizado para efectuar una Transacción, de acuerdo con las Normas. Una Aplicación de Pago de MasterCard, una Aplicación de Pago de Maestro y una Aplicación de Pago de Cirrus constituyen una Aplicación de Pago.

Facilitador de pagos

Un Proveedor de Servicios inscrito por un Adquiriente para facilitar la adquisición de las Transacciones de los Comercios Secundarios por parte del Adquiriente y que efectúa uno o más de los servicios descritos en la Regla 7.1 del manual *Reglamento de MasterCard* como un Servicio del Programa PF.

Terminal En Sucursales basada en PIN

Un dispositivo atendido por personal, ubicado en las instalaciones de un Cliente u otra institución financiera designada como su agente autorizado por la Corporación, que facilita la Transacción de retiro de efectivo del Tarjetahabiente.

Punto de Interacción (POI)

La ubicación en la cual ocurre la Transacción según lo determina la Corporación.

Terminal del Punto de Venta (POS)

Un dispositivo con atención o sin atención de personal ubicado en las instalaciones de un Comercio que permite a un Tarjetahabiente efectuar una Transacción con una Tarjeta y/o Dispositivo de Acceso, para la compra de productos o servicios vendidos por dicho Comercio, de acuerdo con las Normas de seguridad de la Terminal de POS y otras Normas aplicables.

Point–of–Sale (POS) Transaction

The sale of products or services by a Merchant to a Cardholder pursuant to acceptance of a Card by the Merchant. A POS Transaction may be a Card-present Transaction taking place in a face-to-face environment or at an unattended POS Terminal, or a Card-not-present Transaction taking place in a non-face-to-face environment (for example, an e-commerce, mail order, phone order, or recurring payment Transaction).

Portfolio

All Cards issued bearing the same major industry identifier, BIN/IIN, and any additional digits that uniquely identify Cards for routing purposes.

Cliente Principal, Principal

Un Cliente que participa directamente en la Actividad por medio del uso de sus BIN/IIN asignados y que puede Patrocinar uno o más Afiliados.

Transacción Procesada

Una Transacción para la cual:

- (i) el Emisor o su agente aprobó la solicitud del Adquiriente para completar la Transacción ("autorización")por medio del Sistema de Intercambio, o (ii) la autorización en línea no fue requerida conforme con las Normas (por ejemplo, se efectuó una Transacción con Chip que fue menor o igual que el límite de piso del chip aplicable y tanto la Terminal como el chip aprobaron una autorización fuera de línea); y

- El Adquiriente utilizó el Sistema de Intercambio para enviar los datos del registro de la Transacción al Emisor ("compensación") con el fin de transferir fondos ("liquidación") a través del Sistema de Intercambio.

Programa

Programa de emisión de Tarjetas del Cliente, programa de adquisición del Comercio, programa de adquisición de la Terminal de ATM, programa de Actividad Digital, o todos.

Servicio del Programa

Cualquier servicio descrito en la Regla 7.1 del manual *Reglamento de MasterCard* o en otra parte de las Normas que directa o indirectamente apoya un Programa, independientemente de si la entidad que proporciona el servicio está inscrita como un Proveedor de Servicios de uno o más Clientes. La Corporación tiene el derecho exclusivo de determinar si un servicio es un Servicio del Programa.

Región

Una región geográfica según lo definido por la Corporación regularmente. *Consulte* el Apéndice A del manual *Reglamento de MasterCard*.

Transacción a Distancia

Una Transacción del POS que no es cara a cara desarrollada parcialmente o en su totalidad mediante comunicación electrónica, como un pedido telefónico, Internet, mensaje de texto, fax o similar.

Reglamento

Las Normas establecidas en el manual.

Proveedor de Servicios

Una persona que realiza un Servicio del Programa. La Corporación tiene el derecho exclusivo de determinar si una persona es o puede ser un Proveedor de Servicios y, si es así, la categoría del Proveedor de Servicios. Un Proveedor de Servicios es un agente del Cliente que recibe o de otra manera se beneficia del Servicio del Programa, ya sea directa o indirectamente, desarrollado por dicho Proveedor de Servicios.

Facilitador de Inscripción del Proveedor de Servicios

Un Proveedor de Servicios que realiza los servicios de identificación e inscripción del Proveedor de Servicios.

Obligación de Liquidación

Una obligación financiera de un Cliente Principal o Asociación a otro Cliente Principal o Asociación que surja de una Transacción.

Transacción de Depósito Compartido

Un depósito en una Cuenta de ahorros o Cuenta corriente efectuado en una Terminal de ATM ubicada en la Región de EE. UU., iniciado con una Tarjeta emitida por un Cliente de la Región de EE. UU. que no es el Adquiriente y procesada a través de la Red de ATM de MasterCard.

Solicitación, Solicitar

Una aplicación, publicidad, promoción, comunicación de mercadeo, o similar que tiene el propósito de solicitar la inscripción de una persona como Tarjetahabiente o como Comercio. "Solicitar" significa usar una Solicitud.

Programa Especial del Emisor

Actividad del Emisor que la Corporación considera que debe ser realizada sólo con el consentimiento explícito previo de la Corporación. A partir de la fecha de publicación de estas Reglas, los Programas Especiales del Emisor incluyen los Programas de Tarjeta de Afinidad, los Programas de Tarjetas de Coparticipación de Marcas y el Programa de Tarjeta Prepagada y con respecto a la Actividad de MasterCard solamente, la Transacción del Valor de la Marca y Cuenta Propia, la cuenta de Transacción a Distancia de MasterCard y los Programas garantizados de MasterCard.

Patrocinador, Patrocinio

La relación descrita en las Normas entre un Principal o Asociación y un Afiliado que participa en la Actividad indirectamente a través del Principal o la Asociación. En ese caso, el Principal o la Asociación es el Patrocinador del Afiliado y el Afiliado es el Patrocinado por el Principal o la Asociación. "Patrocinio'' significa Patrocinar a un Cliente.

Billetera Digital por Etapas

Funcionalidad mediante la cual el Operador de Billetera Digital por Etapas efectúa un pago en dos etapas a un minorista para completar una compra iniciada por un consumidor, como sigue:

- **Etapa de pago**—En la etapa de pago, el DWO por Etapas paga al minorista por medio de:
  - Una transacción realizada usando datos de una Cuenta de MasterCard o Maestro, o de otra cuenta, asignados al consumidor por el DWO o por un emisor que actúa en nombre o por cuenta del DWO (en este documento, una "cuenta de pago asignada a un consumidor"); o
  - Una transferencia de fondos a una cuenta mantenida por el DWO por Etapas en nombre o por cuenta del minorista.
- **Etapa de provisión de efectivo**—En la etapa de provisión de efectivo, el DWO Por Etapas usa los datos de una cuenta de MasterCard o Maestro, o de otra cuenta, proporcionados al DWO por Etapas por el consumidor (en este documento, la "cuenta de provisión de efectivo") para realizar una transacción que provea efectivo o reembolse a la Billetera Digital por Etapas.

Ni el minorista ni, si el minorista es un Comercio, su Adquiriente o el Proveedor de Servicios del Adquiriente reciben los datos de la Cuenta de MasterCard o Maestro ni otra información que identifique la marca de la red y el emisor de la tarjeta de pago para la cuenta de provisión de efectivo.

Operador de Billetera Digital (DWO) por Etapas

El operador de una Billetera Digital por Etapas.

Normas

Los documentos organizativos, las reglas operativas, las regulaciones, las políticas y los procedimientos de la Corporación, incluyendo, entre otros, los manuales, las guías o los boletines, según sean enmendados cada tanto.

Parámetros del Stand-In

Un conjunto de requisitos de autorización establecido por la Corporación o por el Emisor al que el Sistema de Intercambio tiene acceso usando el Servicio del Procesamiento Stand-In para determinar las respuestas adecuadas a las solicitudes de autorización.

Servicio del Procesamiento Stand-In

Un servicio que ofrece la Corporación en el cual el Sistema de Intercambio autoriza o rechaza Transacciones en nombre de y usa los Parámetros del Stand-In proporcionados por el Emisor (o en algunos casos, por la Corporación). El Procesamiento Stand-In responde solamente cuando el Emisor no está disponible, la Transacción no puede ser entregada al Emisor, o el Emisor se excede de los parámetros de tiempo de respuesta establecidos por la Corporación.

Sublicenciatario

Una persona autorizada por escrito a usar una Marca tanto por un Licenciatario de acuerdo con las Normas como por la Corporación.

Comercio secundario

Un comercio que, conforme a un convenio con el Facilitador de Pagos, está autorizado a aceptar Tarjetas si se presentan adecuadamente.

Convenio de Comercio Secundario

Un convenio entre un Comercio Secundario y un Facilitador de Pagos en el que se establecen los términos en virtud de los cuales se autoriza al Comercio Secundario a aceptar Tarjetas.

Terminal

Any attended or unattended device that meets the Corporation requirements for the electronic capture and exchange of Card data and that permits a Cardholder to effect a Transaction in accordance with the Standards. An ATM Terminal, PIN-based In-Branch Terminal, and POS Terminal is each a type of Terminal.

Procesador Tercero (TPP)

Un Proveedor de Servicios que efectúa uno o más de los servicios descritos en la Regla 7.1 del manual *Reglamento de MasterCard* como un Servicio del Programa de TPP.

Token

Valor numérico que (i) es un sustituto para el número de cuenta primario (PAN) utilizado por el emisor de una tarjeta de pago para identificar una cuenta de tarjeta de pago; (ii) es emitido conforme a la Estructura de Trabajo Técnica de las Especificaciones de Tokenización de Pago de EMV; y (iii) pasa las reglas básicas de validación de un PAN, incluyendo la Fórmula Luhn para Computar el Dígito de Verificación de Módulo 10. Vea también Token de MasterCard.

Tokenización, Tokenizar

Proceso por el cual un Token de MasterCard reemplaza un PAN de la Cuenta.

Solicitante de Token

Una entidad que solicita el reemplazo de PAN de la Cuenta con Token de MasterCard. Vea Solicitante de Token de Billetera.

Caja Fuerte de Token

Un repositorio de token implementados por un sistema de tokenización, que también puede realizar la validación criptográfica y la relación al número de cuenta primario (PAN).

Transacción

Una transacción financiera que surge de la aceptación correcta de una Tarjeta o Cuenta que lleva o que está identificada con una o más de las Marcas Principales, ya sea sola o en combinación con las marcas de otro esquema de pago, en una ubicación de aceptación de Tarjeta y que se identifica en los mensajes con un identificador del Programa de Tarjeta.

Sistema de Manejo de las Transacciones

Efectúa los servicios de manejo de las Transacciones para los Pagos de MasterCard Basados en la Nube, que pueden incluir la autenticación de la credencial, la relación y validación del criptograma de la aplicación, asegurar la sincronización con el Sistema de Manejo de Credenciales y enviar las Transacciones al Emisor para la autorización.

Gerente de Servicios Confiable

Provee el elemento seguro de un Dispositivo de Acceso con la Aplicación de Pago, los datos de personalización o los comandos de manejo de la aplicación después de la emisión mediante un canal de comunicación inalámbrico (OTA).

Volumen

El valor financiero agregado de un grupo de Transacciones. "Volumen" no significa el número de Transacciones.

Proveedor de Billetera

Vea Solicitante de Token de Billetera.

Solicitante de Token de Billetera

Un DWO que, a solicitud de un Tarjetahabiente para la Digitalización, incluyendo Tokenización, de un PAN de la Cuenta, invoca la Identificación y Verificación (ID&V) y el Enlace de Dispositivo; denominado también un "Proveedor de Billetera" . Un Solicitante de Token de Billetera es un tipo de Solicitante de Token.

Palabra Registrada

Una Marca que consiste en el nombre de las marcas de la Corporación seguido de una marca comercial registrada ® o ™ símbolo (según el estado de su marca comercial en un país particular) o el equivalente de la ley local. *Vea* Marca Registrada de Cirrus, Marca Registrada de Maestro, Marca Registrada MasterCard.

Notices

Proprietary Rights

The information contained in this document is proprietary and confidential to MasterCard International Incorporated, one or more of its affiliated entities (collectively "MasterCard"), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

Trademarks

Trademark notices and symbols used in this document reflect the registration status of MasterCard trademarks in the United States. Please consult with the Global Customer Service team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Disclaimer

MasterCard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, MasterCard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not MasterCard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, MasterCard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

Translation

A translation of any MasterCard manual, bulletin, release, or other MasterCard document into a language other than English is intended solely as a convenience to MasterCard customers. MasterCard provides any translated document to its customers "AS IS" and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall MasterCard be liable for any damages resulting from reliance on any translated document. The English version of any MasterCard document will take precedence over any translated version in any legal proceeding.

Information Available Online

MasterCard provides details about the standards used for this document—including times expressed, language use, and contact information—on the Publications Support page available on MasterCard Connect™. Go to Publications Support for centralized information.