Los Ataques de Skimming en Cajeros Automáticos y Cómo Prevenirlos

Mario Rivero
Director, Investigación de Fraudes
Visa Inc.

Franz Gottschalk
Gerente de Programa, Seguridad del PIN, Las Américas
Visa Inc.

Aviso sobre la Confidencialidad

Esta presentación se le proporciona únicamente en su capacidad de cliente de Visa Inc. y/o participante en el sistema de pago Visa. Al aceptar esta presentación, usted reconoce que la información contenida en el presente documento (la "Información") es confidencial y está sujeta a las restricciones relacionadas con la confidencialidad delineadas en los reglamentos operativos de Visa y/o en otros acuerdos de confidencialidad, los cuales limitan el uso de la Información por parte de usted. Usted conviene en mantener la Información con estricto carácter confidencial y en no utilizar la Información para ningún propósito que no sea en su capacidad como cliente de Visa Inc. o participante en el sistema de pago Visa. La Información se puede diseminar únicamente dentro de su organización de acuerdo con la necesidad de conocerla para habilitar su participación en el sistema de pago Visa. Se le advierte que la Información podría constituir información interna fundamental no pública bajo las leyes federales que regulan los títulos valores en Estados Unidos, y que la compra o venta de títulos valores de Visa Inc. mientras se tiene conocimiento de información interna fundamental no pública constituiría una violación de las leyes federales aplicables de Estados Unidos que regulan los títulos valores.

Renuncia de Responsabilidad

La información, recomendaciones o "mejores prácticas" contenidas en el presente se proporcionan "TAL CUAL ESTÁN", son mero título informativo y no deberá dependerse de ellas para asesoramiento operativo, de mercadeo, legal, técnico, impositivo, financiero o de otro tipo. Al implementar una estrategia o práctica nueva, deberá consultar con su asesor legal a fin de determinar qué leyes y reglamentaciones son de aplicación según sus circunstancias específicas. Los costos, ahorros y beneficios reales de toda recomendación, programa o "mejor práctica" variarán basado en sus necesidades comerciales y requisitos de programas específicos. Por su naturaleza, las recomendaciones no son garantía de desempeño o resultados futuros y están sujetas a riesgos, incertidumbres y presunciones difíciles de predecir o cuantificar. Nuestras presunciones se hicieron a la luz de nuestra experiencia y percepción de tendencias históricas, condiciones actuales, desarrollos futuros esperados y demás factores que consideramos apropiados según las circunstancias. Las recomendaciones están sujetas a riesgos y a incertidumbres, que podrían hacer que los resultados y tendencias reales y futuros difieran materialmente de las presunciones o recomendaciones. Visa no es responsable por el uso que usted haga de la información contenida en el presente (incluidos errores, omisiones, imprecisiones o falta de oportunidad de cualquier tipo), como así tampoco de presunción o conclusión alguna que usted pudiere inferir de su uso. Visa no otorga garantía alguna, expresa o implícita, y expresamente renuncia a las garantías de comerciabilidad y de adecuacidad de uso para un propósito en particular, a toda garantía de no violación de los derechos de propiedad intelectual de un tercero, a toda garantía de cumplimiento de la información con los requisitos de un cliente o a toda garantía de actualización de la información y de información sin errores. Hasta el grado permitido por la ley de aplicación, Visa no será tenida como responsable ante un cliente o un tercero por daños y perjuicios conforme a teoría alguna de derecho, incluido sin limitaciones, todo daño especial, emergente, incidental o punitivo, como así tampoco por daños y perjuicios por lucro cesante, interrupción de los negocios, pérdida de información comercial u otra pérdida monetaria, incluso si fuere notificada de la posibilidad de dichos daños y perjuicios.

Aviso sobre la Confidencialidad

Esta presentación se le proporciona únicamente en su capacidad de cliente de Visa Inc. y/o participante en el sistema de pago Visa. Al aceptar esta presentación, usted reconoce que la información contenida en el presente documento (la "Información") es confidencial y está sujeta a las restricciones relacionadas con la confidencialidad delineadas en los reglamentos operativos de Visa y/o en otros acuerdos de confidencialidad, los cuales limitan el uso de la Información por parte de usted. Usted conviene en mantener la Información con estricto carácter confidencial y en no utilizar la Información para ningún propósito que no sea en su capacidad como cliente de Visa Inc. o participante en el sistema de pago Visa. La Información se puede diseminar únicamente dentro de su organización de acuerdo con la necesidad de conocerla para habilitar su participación en el sistema de pago Visa. Se le advierte que la Información podría constituir información interna fundamental no pública bajo las leyes federales que regulan los títulos valores en Estados Unidos, y que la compra o venta de títulos valores de Visa Inc. mientras se tiene conocimiento de información interna fundamental no pública constituiría una violación de las leyes federales aplicables de Estados Unidos que regulan los títulos valores.

Skimming

- El skimming es un método que utilizan los delincuentes para capturar los datos codificados en la banda magnética en el reverso de una tarjeta.
- Lo hacen utilizando dispositivos físicos o equipos.
- El objetivo es capturar o “skim” la información codificada en la banda magnética para después producir tarjetas clonadas con el fin de utilizarlas en forma fraudulenta.
- El skimming no se refiere a la creación de una tarjeta falsificada o clonada, sino al acto de robar la información o datos de la tarjeta.

El Skimming en los Cajeros Automáticos

El skimming en los cajeros automáticos es un método que usan los delincuentes para capturar los datos de la banda magnética mientras la tarjeta se está usando en el cajero automático.

Los delincuentes utilizan diversos métodos y dispositivos para robar los datos de la cuenta de la tarjeta Y TAMBIÉN el PIN (o NIP) del cliente.

Teniendo ya en sus manos los datos completos de la pista de la banda magnética y los PINes, los delincuentes producen entonces tarjetas clonadas y las distribuyen a corredores que son empleados por grupos organizados con el objetivo de sacar dinero de las cuentas de los tarjetahabientes.

Para poder perpetrar el skimming con éxito, se requieren un dispositivo llamado “skimmer” y un dispositivo para capturar el PIN.

Diversos Métodos de Skimming

Dispositivos de Skimming

- "Skimmers" – Dispositivos fabricados a la medida para almacenar datos, los cuales se usan para robar los datos codificados en la pista de la banda magnética de tarjetas genuinas.
- Diseñados para se puedan colocar sobre la abertura o "boca" del lector de tarjetas del cajero automático. Se fabrican frentes o paneles falsos que cubren toda la superficie del frente del lector de tarjetas.
- Diseñados para que parezca que son parte del cajero automático.

Diversos Métodos para Capturar el PIN

Panel Falso con Cámara

Cámara Estenopeica

Cámara Estenopeica

- El método más sofisticado y más ampliamente utilizado.
- Consiste en instalar una cámara estenopeica cerca del cajero automático, la cual graba en video al tarjetahabiente mientras ingresa su PIN.
- La imagen de video se almacena o transmite a un dispositivo receptor situado a un máximo de cien metros.

Diversos Métodos para Capturar el PIN

Teclado de PIN Falso

- Se coloca sobre el teclado de PIN legítimo.
- El perpetrador del fraude se hace pasar por un técnico y altera el teclado de PIN implantando un dispositivo para capturar los PINes que ingresen los tarjetahabientes.

Espiar al Usuario por encima del Hombro

- Los PINes se obtienen espiando por encima del hombro a la víctima del fraude mientras está ingresando su PIN.
- Método poco tecnológico que es, sin embargo, muy efectivo.

Otros Métodos para Robar Tarjetas en Cajeros Automáticos

Distraer al Usuario

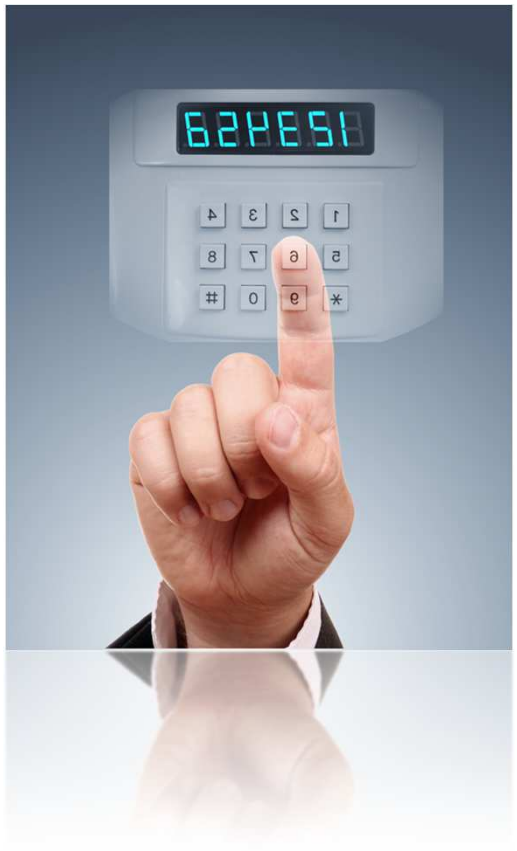
- El perpetrador del fraude provoca algún tipo de situación para distraer el tarjetahabiente.
- El skimming se realiza entonces utilizando un dispositivo de mano mientras el tarjetahabiente está distraído.

El "Buen Samaritano"

- Utilizando una banda o manga de metal o plástico, se bloquea la ranura que dispensa el efectivo en el cajero automático.
- Cuando el cajero no dispensa los fondos, el "Buen Samaritano" sugiere ingresar de nuevo el PIN mientras él o ella observa.
- La máquina retiene la tarjeta insertada.
- El perpetrador del fraude la recupera después que el tarjetahabiente se marcha.

Diversos Métodos de Skimming

Ataques de Malware



- El malware es la nueva tendencia en los ataques para robar datos de tarjetas en cajeros automáticos.
- El atacante puede implantar el malware después de comprometer la seguridad del cajero automático físico o del software que hace funcionar la máquina.
- Algunos tipos de malware que específicamente se usan en los cajeros automáticos no solamente son capaces de capturar los datos del tarjetahabiente, sino que también le dan al atacante la habilidad de dispensar efectivo y elegir la denominación de billetes que desean dispensar.

PREVENCIÓN

Prevención del Skimming en Cajeros Automáticos

- Inspecciones regulares de cajeros automáticos
- Implementación de controles de Adquirente

Prevención del Fraude en Cajeros Automáticos

- Consideraciones del Adquirente
- Consideraciones del Emisor

Migración a Tarjetas de Chip y Cajeros Automáticos EMV

Prevención del Skimming en Cajeros Automáticos

Realizar Inspecciones Regulares de los Cajeros Automáticos

- Inspecciones físicas de rutina cada vez que se reponga el efectivo o durante los mantenimientos. Se recomienda hacer inspecciones al azar.
- Fijarse bien en cualquier aviso colocado en los cajeros automáticos que no esté autorizado por el banco.
- Inspeccionar para detectar cualquier señal de alteración o cualquier accesorio o dispositivo pegado o instalado en los cajeros automáticos:
  - Paneles falsos o partes o accesorios flojos, para asegurar que no se haya instalado ninguna cámara estenopeica o dispositivo de grabación
  - Cables sueltos o flojos cerca del teclado de PIN o en la cubierta externa del cajero automático
  - Inspeccionar la ranura del lector de tarjetas para detectar cualquier equipo o dispositivo no autorizado o cualquier señal de alteración, como residuos de pegamentos o adhesivos.
  - Fijarse en cualquier objeto, cubierta o caja que sobresalga del cajero y desde el cual se pueda ver directamente el teclado de PIN, y que se pudiera utilizar para instalar una cámara.
- Fortalecer la seguridad del sistema operativo y software de los cajeros automáticos.

VISA

Prevención del Skimming en Cajeros Automáticos

Implementación de Controles de Adquirente

- Instalar cámaras de televisión de circuito cerrado (CCTV) en todas las ubicaciones donde haya cajeros automáticos, siempre que sea posible.
- Equipar los cajeros automáticos con características "anti-skimming" :
  - Lector de Tarjetas "Jitter" (de efecto vibratorio)
  - Panel Anti-Skimmer – Ayuda a evitar que el perpetrador coloque un dispositivo de skimming encima de la ranura donde se inserta la tarjeta en el cajero automático
  - Dispositivo emisor de interferencias de frecuencias radiales que distorsione el campo electromagnético que rodea al lector de tarjetas
- Advertirles a los clientes que deben mantenerse alerta y observar el cajero automático para detectar cualquier tipo de accesorio o aditamento "inusual" en el mismo.
- Tener la capacidad de recuperar de inmediato las cuentas dentro de cualquier plazo o máquina de cajero automático que se especifique, a fin de facilitar alertas a los miembros si se ha comprometido la seguridad.

Prevención del Skimming en Cajeros Automáticos

Consideraciones del Adquirente

- Colocar cámaras de televisión de circuito cerrado que sirvan como un freno para disuadir a posibles delincuentes y faciliten las investigaciones por parte de la policía.
- Recuperar las imágenes de las cámaras de televisión de circuito cerrado que correspondan a retiros de efectivo confirmados como fraudulentos en el cajero automático, a fin de facilitar la investigación.
- Monitorear en tiempo real para detectar actividades sospechosas en cuentas que tengan lugar en los cajeros automáticos:
  - Consulta de saldo, retiro y/o cambio de PIN que ocurran en forma subsiguiente en más de una cuenta dentro de un plazo de tiempo breve
  - Retiros repetidos y/o intentos de declinación en varias cuentas dentro de un plazo de tiempo breve

Prevención del Fraude en Cajeros Automáticos

Consideraciones del Emisor

- Establecer límites diarios de efectivo y número de retiros por tarjeta para la actividad en los cajeros automáticos.
- Enviar mensajes de texto de alerta al teléfono celular (por ejemplo, Alertas de Transacción de Visa) del cliente para varios tipos de retiros.
- Monitorear en tiempo real para detectar cualquier actividad sospechosa en los cajeros automáticos (por ejemplo, V.I.P y Vital Signs):
  - Consulta de saldo, retiro y/o cambio de PIN que ocurran en forma subsiguiente
  - Retiros sucesivos por montos altos y/o intentos de declinación en las cuentas
- Investigar todas las quejas de los clientes para determinar si podrían deberse al skimming o compromiso de la seguridad en un cajero automático.
- Alertar a las autoridades locales y a Visa de inmediato en caso de sospechar que ha ocurrido un incidente relacionado con el skimming.

Migración a Tarjetas de Chip y Cajeros Automáticos EMV

- Al introducir valores dinámicos para cada transacción, la tecnología de chip EMV reduce considerablemente la habilidad de un delincuente para utilizar datos robados de tarjetas de pago.
- Cambio en la Responsabilidad relacionado con EMV
  - Visa ha establecido un plazo para animar a los Adquirentes a mejorar los cajeros automáticos a fin de que acepten tarjetas de chip EMV.
  - La responsabilidad por los fraudes relacionados con tarjetas falsificadas utilizadas en cajeros automáticos se asignará a la parte – Adquirente o Emisor – que no haya adoptado la tecnología de chip EMV.
  - Si se usa una tarjeta de chip EMV en un cajero que no tenga la capacidad de aceptar tarjetas de chip EMV, el Adquirente del cajero automático asumirá el costo del fraude debido al uso de una tarjeta falsificada.
  - El fraude se puede prevenir si tanto el Emisor como el Adquirente usan la tecnología de chip y/o PIN EMV.

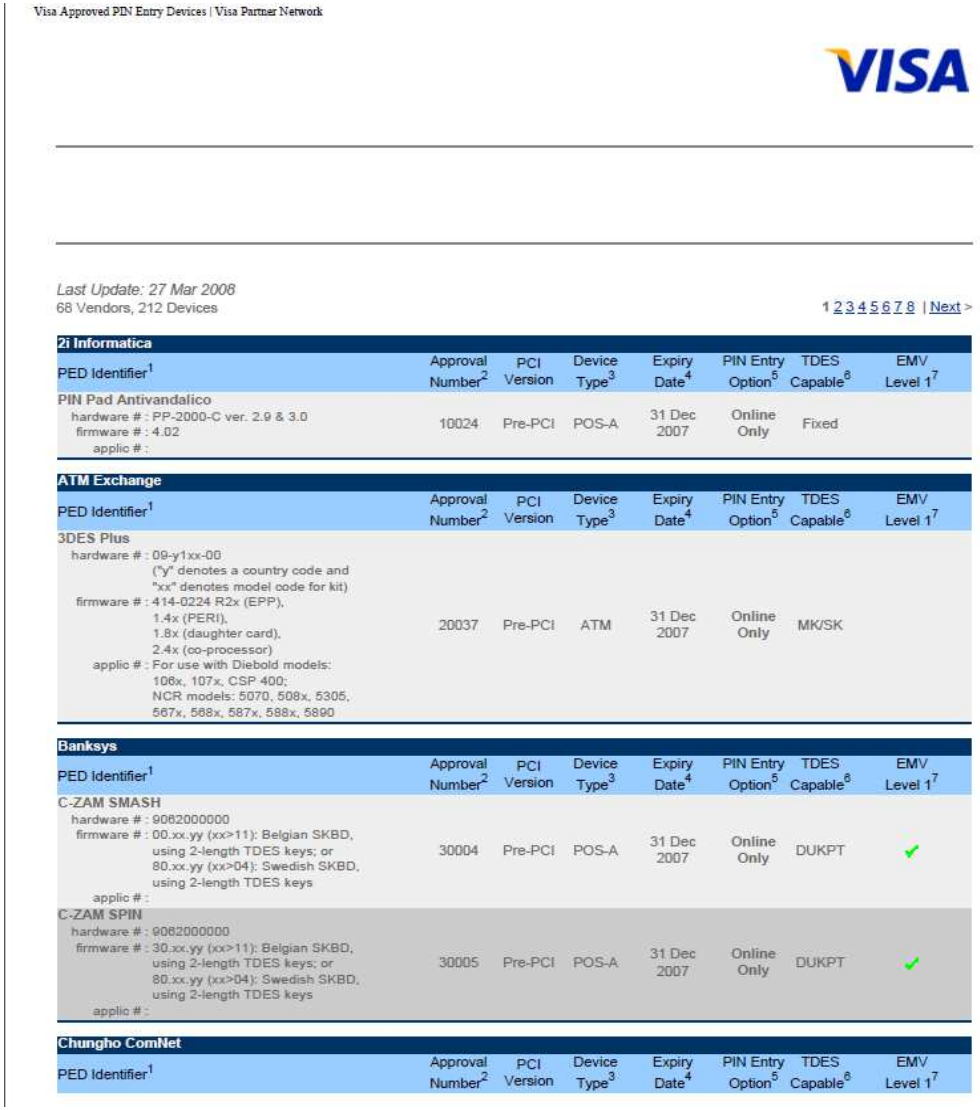
Programa de la Seguridad de PIN Visa

Garantizar la seguridad y solidez de los pagos electrónicos para respaldar su permanente crecimiento

Listado de Dispositivos de PIN Pre-PCI

Reglas de uso Pre-PCI PED

- Lista completa de dispositivos que están expirados
- Los EPPs expirados no pueden ser comprados o hacer nuevas instalaciones con ellos
- No tienen fecha de caducidad hasta el momento
- La lista de dispositivos Pre-PCI PIN esta en www.visa.com/pin



Visa Approved PIN Entry Devices | Visa Partner Network

VISA

Last Update: 27 Mar 2008
68 Vendors, 212 Devices

1 2 3 4 5 6 7 8 | Next >

2i Informatica

PED Identifier[1]	Approval Number[2]	PCI Version	Device Type[3]	Expiry Date[4]	PIN Entry Option[5]	TDES Capable[6]	EMV Level 1[7]
PIN Pad Antivandalico hardware # : PP-2000-C ver. 2.9 & 3.0 firmware # : 4.02 applic # :	10024	Pre-PCI	POS-A	31 Dec 2007	Online Only	Fixed	

ATM Exchange

PED Identifier[1]	Approval Number[2]	PCI Version	Device Type[3]	Expiry Date[4]	PIN Entry Option[5]	TDES Capable[6]	EMV Level 1[7]
3DES Plus hardware # : 09-y1xx-00 ("y" denotes a country code and "xx" denotes model code for kit) firmware # : 414-0224 R2x (EPP), 1.4x (PERI), 1.8x (daughter card), 2.4x (co-processor) applic # : For use with Diebold models: 106x, 107x, CSP 400; NCR models: 5070, 508x, 5305, 567x, 568x, 587x, 588x, 5890	20037	Pre-PCI	ATM	31 Dec 2007	Online Only	MK/SK	

Banksys

PED Identifier[1]	Approval Number[2]	PCI Version	Device Type[3]	Expiry Date[4]	PIN Entry Option[5]	TDES Capable[6]	EMV Level 1[7]
C-ZAM SMASH hardware # : 9062000000 firmware # : 00.xx.yy (xx>11): Belgian SKBD, using 2-length TDES keys; or 80.xx.yy (xx>04): Swedish SKBD, using 2-length TDES keys applic # :	30004	Pre-PCI	POS-A	31 Dec 2007	Online Only	DUKPT	✔
C-ZAM SPIN hardware # : 9062000000 firmware # : 30.xx.yy (xx>11): Belgian SKBD, using 2-length TDES keys; or 80.xx.yy (xx>04): Swedish SKBD, using 2-length TDES keys applic # :	30005	Pre-PCI	POS-A	31 Dec 2007	Online Only	DUKPT	✔

Chungho ComNet

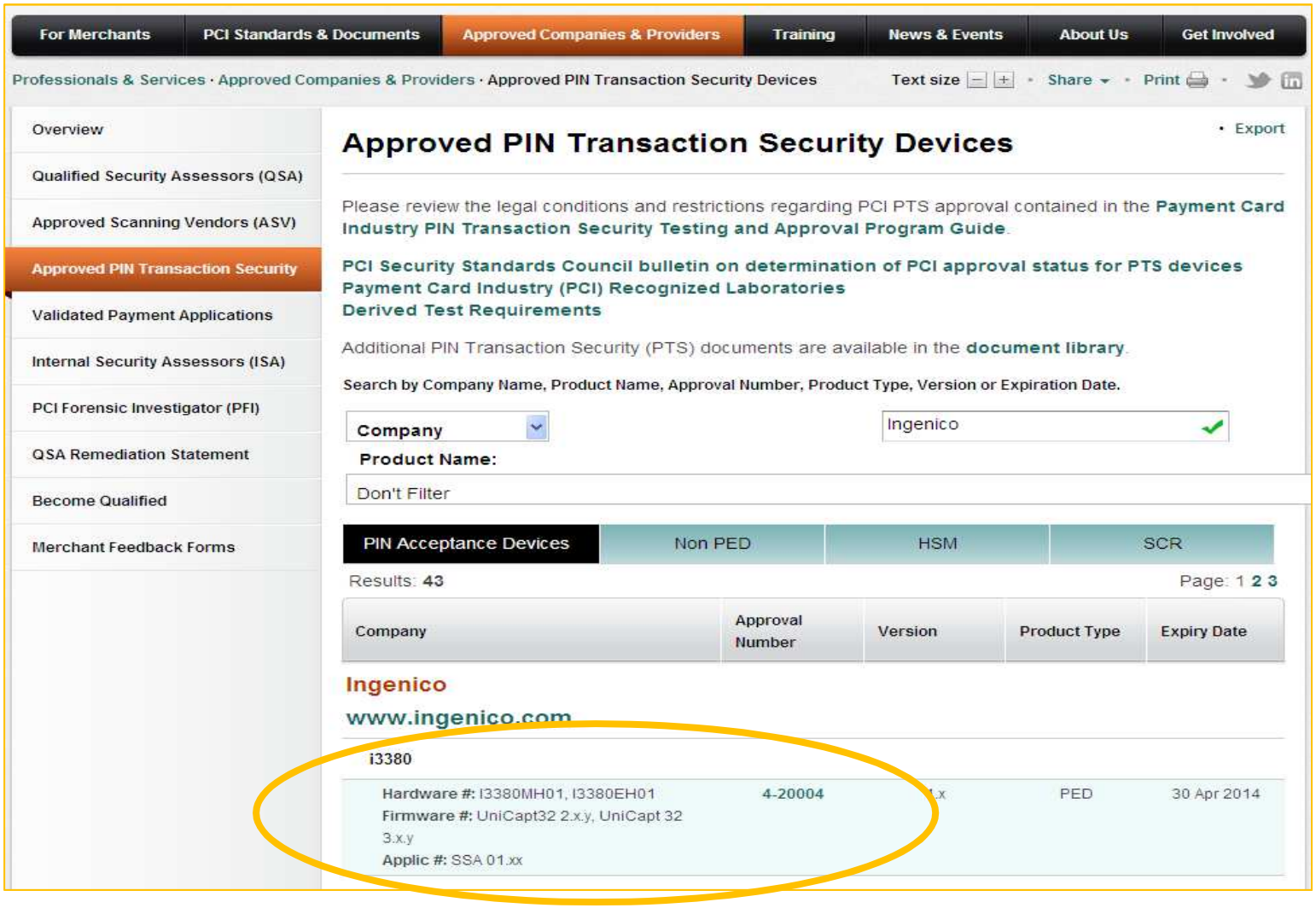
PED Identifier[1]	Approval Number[2]	PCI Version	Device Type[3]	Expiry Date[4]	PIN Entry Option[5]	TDES Capable[6]	EMV Level 1[7]

www. visa.com/pin - 02/21/14

VISA

Dispositivos de Seguridad de Transacciones con PIN Aprobados por PCI

Siempre valide el Hardware, el Firmware y la Aplicación antes de realizar una compra



www.pcisecuritystandards.org - 02/21/14

Como Prevenir el Fraude Mediante los Requerimientos de la Seguridad del PIN PCI

Amenazas en el Dispositivo

Amenazas	Defensas
PED alterados	• Requisito de Seguridad del PIN n.º 29
Diseño que no cumple con las normas	• Certificación de laboratorio/Especificaciones de diseño del dispositivo
Llaves que no son únicas	• Requisito de Seguridad del PIN n.º 20
Fallas en la gestión de llaves	• Requisito de Seguridad del PIN (varios)
Ataque de diccionario	• Requisito de Seguridad del PIN n.º 3
Exposición a riesgo visual	• Certificación de laboratorio/Especificaciones de diseño del PED; Requisito de Seguridad del PIN n.º 29

VISA

Como Prevenir el Fraude Mediante los Requerimientos de la Seguridad del PIN PCI

Amenazas en un Servidor de Adquirente

Amenazas	Defensas
Registro de los PIN/datos del tarjetahabiente	• Requisito de Seguridad del PIN n.º 4/PCI-DSS
Prácticas inapropiadas	• Aplicaciones que cumplen con PCI PA-DSS
Ausencia de control de cambios	• PCI DSS / Anexo Normativo A
Control del equipo	• Requisitos de Seguridad del PIN n.º 29, n.º 30 y n.º 31
Fallas en la gestión de llaves	• Requisitos de Seguridad del PIN (varios)
Llaves de producción en prueba	• Requisito de Seguridad del PIN n.º 19
HSM mal configurado	• Depuración de comando del HSM

Como Prevenir el Fraude Mediante los Requerimientos de la Seguridad del PIN PCI

Amenazas en ESO

Amenazas	Defensas
Prácticas inapropiadas de carga de llaves	• Requisitos de Seguridad del PIN n.º 12 y n.º 13
Control del equipo	• Requisitos de Seguridad del PIN n.º 29, n.º 30 y n.º 31
Fallas en la gestión de llaves	• Requisitos de Seguridad del PIN (varios)
Adquisiciones Dispositivos inadecuadas	• Requisito de Seguridad del PIN n.º 1 (órdenes PED de Visa)
Uso de ESO sin registrar	• El registro requiere diligencia debida

Como Prevenir el Fraude Mediante los Requerimientos de la Seguridad del PIN PCI

Amenazas en el Switch

Amenazas	Defensas
Falla en la gestión de llaves	• Requisitos de Seguridad del PIN (varios
Control criptográfico de equipos	• Requisito de Seguridad del PIN n.º 31

Como Prevenir el Fraude Mediante los Requerimientos de la Seguridad del PIN PCI

Amenazas en el Emisor

Amenazas	Defensas
Transmisión/envío del PIN	• Programa para Proveedores de Tarjetas Visa
Personalización de Tarjetas	• Programa para Proveedores de Tarjetas Visa
Verificación del PIN	• No hay defensas de PCI. Utilice Visa AA
Suplantación de Identidad	• No hay defensas de PCI
Llaves del Emisor Obsoletas	• No hay requisitos específicos para PCI El sistema VIP tiene DKE
Informe de Fraudes de PIN	• Servicio disponible en la Región LAC desde julio del 2008
HSM mal configurado	• Eliminación de comandos del HSM

Sitio Web del Programa de Seguridad del PIN Actualizado

- Cambios al Programa de Seguridad del PIN Efectivos a partir del 1º de Enero del 2014
- Uso del Dispositivo de Ingreso de PIN (PED), Fechas de Caducidad y Expiración
- Lista de PED Comprometidos

www.visa.com/pinsecurity
02/21/14

PIN Security Program

Visa is simplifying and unifying PIN security compliance validation across all regions.

Welcome to Visa® PIN Security website. The information on this site describes Visa's global Personal Identification Number (PIN) Security program designed to assist organizations in maintaining the highest level of PIN security. This website contains timely *NEWS* articles about PIN topics as well as *Important Visa PIN Information* for anyone involved with PIN processing.

If you have any questions pertaining to PIN security at Visa, contact your regional Visa Risk Representative or send an email to pin@visa.com.

NEWS

Changes to PIN Security Program Go Into Effect - 1 January 2014 *NEW*

Visa is updating its PIN Security Program, simplifying and unifying PIN security compliance validation across all Visa Inc. regions. The modifications will drive PIN security through a risk-based, prioritized approach that focuses on entities that process PIN data or perform key management activities on behalf of Visa clients.

Visa PIN Security Program changes go into effect 1 January 2014.

Read more about the program changes:

- Visa PIN Security Program Modifications
- Visa PIN Security Program FAQ
- Visa PIN Webinar presentation December 2013
  English
  Spanish

For information on the PIN Security Program modifications, contact your regional Visa Risk Representative.

Important Visa PIN Information

PIN Entry Device (PED) Usage, Sunset and Expiration Dates *NEW*

Visa's PIN Entry Device (PED) requirements have been updated.

Know key dates and best practices to consider when developing PED acquisitions, usage and deployment strategies for your organization. Answers to PED frequently asked questions and information about PCI PTS V1.x devices expiring on April 30, 2014 is included.

- **Visa PED Entry Device Requirements**

Compromised PIN Entry Device (PED) List *NEW*

Visa's maintains a list of older **PIN Entry Devices (PED) reported as compromised** and may be vulnerable to attacks.

Top Downloads

Resources

PCI PIN Security Requirements

PCI Point of Interaction (POI) Modular Security Requirements

PCI ATM Security Guidelines PDF | 1.01M

PCI PIN Security Assessment Questionnaire (SAQ) Template DOC | 106k

PCI PIN Security Requirements Auditor's Guide PDF | 774KB

Key Injection Facility Auditor's Guide PDF | 685KB

Listing of Visa Pre-PCI Approved PIN Entry Devices PDF | 268k

Articles

Encrypting PIN Pads Must Be Industry-Approved - PDF–06 December 2012 PDF | 282 KB

Maximize Point-Of-Sale PIN-Entry Device Security–06 December 2012 PDF | 263 KB

Help Protect Cardholder

¿Preguntas?

Gracias