Protección de datos de tarjetas de pago en transacciones presenciales: cómo usar PCI PIN y PCI P2PE para establecer un ecosistema de pagos seguro

Desde los orígenes de las tarjetas de pago (crédito y débito), a mediados del siglo XX, la necesidad de protección contra las diferentes formas de fraude ha sido un elemento clave para garantizar la legitimidad y la confianza necesarias para la aceptación social de este mecanismo de pago. Sin embargo, a pesar de los cambios tecnológicos actuales, el modelo de pago con tarjetas se ha quedado obsoleto en términos de seguridad y expuesto a múltiples riesgos. Es precisamente aquí cuando es necesario estandarizar controles específicos para la protección de estos datos en transacciones presenciales empleando técnicas de seguridad modernas.

David E. Acosta Rodríguez

Breve historia de las tarjetas de pago

En 1949, durante una cena en el restaurante "Major's Cabin Grill" (ubicado justo al lado del icónico edificio "Empire State" en Nueva York), Frank X. McNamara (de la "Hamilton Credit Corporation"), Ralph Sneider (abogado del Sr. McNamara) y Alfred Bloomingdale (nieto del fundador de "Bloomingdale's", una cadena de establecimientos de artículos de lujo) estaban hablando acerca de un cliente del Sr. McNamara que tenía problemas económicos para hacer frente a sus deudas. De forma irónica, ese día Frank McNamara había olvidado su billetera en casa y no tenía dinero para pagar la cena, teniendo que llamar a su esposa para que le ayudara[1].

Debido a la vergüenza que le generó esta situación, juró que no volvería a pasar por ello e ideó un sistema que evitaba el uso de dinero en efectivo empleando una tarjeta vinculada a un cupo de crédito. Tiempo más tarde, en 1950, estas mismas tres personas fundaron "The Diners' Club" ("El club de cenadores") ofreciendo a los restaurantes una serie de tarjetas con acceso a créditos que implicaban una pequeña cuota de mantenimiento al titular y una comisión al establecimiento por cada transacción realizada.

Este mismo modelo empezó a ser usado por los bancos y fue así como en 1958 el "Bank of America" puso en circulación su tarjeta "BankAmericard" (más tarde renombrada como "VISA"), la "American Express Company" hizo lo mismo con su tarjeta "American Express" y más tarde, en 1966, un grupo de bancos de California denominado "Interbank Card Association" emitieron su tarjeta propia, denominada "Master Charge", posteriormente renombrada como "MasterCard".

Figura 1.- Imagen de las primeras tarjetas Diner's Club, American Express, BankAmericard (posteriormente VISA) y Master Charge (posteriormente MasterCard).

Al principio, estas tarjetas eran de papel. Posteriormente, empezaron a migrar hacia el plástico por motivos de durabilidad. Hacia 1969 se empezó a usar la banda magnética para optimizar la lectura de los datos de las tarjetas a través de medios electromecánicos. En 1964 se diseñó el primer dispensador de dinero o cajero automático ("*Automated Teller Machine*" – ATM) y en 1973 ya se podían hacer pagos en máquinas de puntos de venta ("Point-of-Sale" – POS).

En 1967 se puso en marcha un mecanismo que permitía autenticar al titular de la tarjeta con un número secreto denominado "Número de Identificación Personal" ("*Personal Identification Number*" – PIN) para remplazar la firma manuscrita. En 1989 la ISO/IEC publicó el estándar ISO/IEC 7812 que estandarizaba los números de cuenta primarios ("*Personal Account Number*" – PAN) asociados a cada tarjeta y en 1986 se empezó a usar en Francia un circuito integrado en la tarjeta que remplazaba los datos de la banda magnética y agregaba nuevas capacidades de seguridad (denominadas "*smart cards*"), que a la larga evolucionaría en los chips EMV (Europay, Mastercard y Visa, las tres compañías que lo estandarizaron).

Con estos datos en mente, es increíble pensar que en el año 2020 aún estemos empleando una tecnología de pagos creada hace más de 70 años y que, a pesar de los cambios tecnológicos que han acompañado estas últimas décadas, no haya evolucionado de forma significativa: seguimos usando un PIN de cuatro dígitos, un número de tarjeta de 16 dígitos y casi la totalidad de tarjetas siguen manteniendo la banda magnética por cuestiones de retrocompatibilidad. De acuerdo con el Banco de España, actualmente hay en nuestro país aproximadamente 85 millones de tarjetas de pago (plásticos) en circulación, más de 60.000 cajeros electrónicos y casi dos millones de terminales de punto de venta[2], lo que nos indica que esta tecnología está lejos de convertirse en obsoleta.

No obstante, no todo es perfecto en este sistema. A medida que pasan los años, las

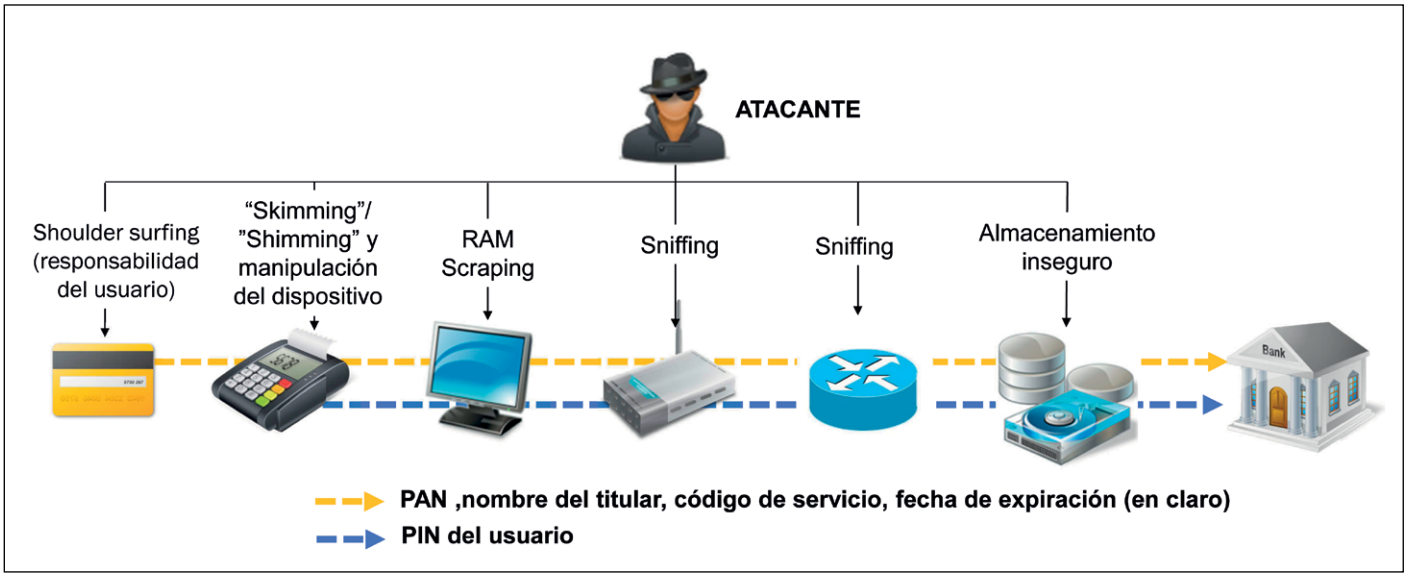

Figura 2.- Enumeración de técnicas para la obtención no autorizada de datos y puntos vulnerables en una transacción con tarjeta de pago.

amenazas que le surjen se vuelven más complejas y los fraudes con tarjetas de pago siguen creciendo. Capital One (106 millones de clientes afectados en 2019), Marriott (500 millones de clientes afectados en 2018), Equifax (143 millones de clientes afectados en 2017), Home Depot (56 millones de tarjetas afectadas en 2014), Target (40 millones de tarjetas afectadas en 2013) y GlobalPayments (1.5 millones de tarjetas afectadas en 2012) son solo algunos ejemplos de cómo los datos de las tarjetas de pago son uno de los principales elementos buscados por delincuentes.

Dentro de las técnicas empleadas para la obtención ilícita de datos de tarjetas de pago por parte de estos delincuentes se pueden enumerar las siguientes:

- **Shoulder sourfing**: Se basa en la observación directa (personalmente) o indirecta (empleando cámaras, binoculares o cualquier otro dispositivo de visualización a distancia) de datos confidenciales de un usuario sin su autorización.
- **Skimming**: Captura no autorizada de los datos de la banda magnética a través de diferentes dispositivos (denominados "skimmers") que emplean las mismas funcionalidades que cualquier lector legítimo y que por lo general son ubicados de forma encubierta para evitar que el usuario detecte su presencia.
- **Shimming**: Una técnica derivada del "skimming" que permite la obtención pasiva de los datos del chip EMV a través de un dispositivo denominado "shim" [3].
- **RAM scraping** (o "memory parsing"): Búsqueda de datos de tarjetas de pago en la memoria temporal de los dispositivos involucrados en los pagos. Esta es una técnica empleada de forma masiva por *malware* para terminales de pago ("POS malware").
- **Sniffing**: Captura del tráfico de las transacciones con tarjetas de pago en busca de datos sensibles.
- Identificación de **repositorios inseguros** con datos de tarjetas de pago en texto claro (archivos, bases de datos, hojas de cálculo, etc.)
- Uso de **dispositivos de pago manipulados u obsoletos** para copiar la información de las transacciones realizadas en él.
- Lectura fraudulenta de datos de tarjeta de pago empleando NFC ("contactless").

Y todo esto solamente en transacciones presenciales (que requieren la presencia física del titular de la tarjeta) sin contar los riesgos asociados a transacciones en comercio electrónico o telefónico.

El reto de proteger de forma segura una tecnología arcaica frente a amenazas actuales

Ahora bien, situados en este punto nos podemos preguntar lo siguiente: si el modelo de pagos con tarjetas es arcaico en términos de seguridad, ¿por qué se sigue usando o por qué no se remplaza por otro modelo más seguro?

La respuesta a esta pregunta se puede dividir en dos argumentos principales:

- Debido a restricciones técnicas y económicas: La adición o modificación de cualquier control de seguridad en el modelo implicaría impactos a gran escala debido a la masificación actual de tarjetas, lectores y otros dispositivos transaccionales. Un ejemplo claro se puede encontrar en la adecuación de las tarjetas de pago con chips EMV en Estados Unidos, en donde existen más de 1.200 millones de tarjetas de pago activas, cerca de ocho millones de terminales de pago y más de 400 mil cajeros electrónicos, lo que ha implicado el remplazo progresivo de todas las tarjetas antiguas con banda magnética y la actualización de dispositivos para soportar esta funcionalidad por un coste de entre 8 mil a 12 mil millones de dólares [4].
- Debido a la adaptación a nuevas tecnologías: La facilidad de uso de las tarjetas de pago (plásticos) ha permitido que el modelo pueda ser empleado por cualquier persona con una curva de aprendizaje mínima. Si se agregan controles adicionales implicará adaptar y reeducar a los usuarios a los nuevos modelos, lo cual conlleva costes y tiempos.

Obviamente, existen actualmente múltiples métodos de pago emergentes ("digital/mobile wallets", criptodivisas, pagos vía QR, etc.) pero tardarán bastante tiempo en convertirse en un modelo que pueda amenazar a los pagos tradicionales con tarjetas. Mientras tanto, es necesario establecer un modelo de seguridad que permita proteger los datos de las tarjetas de pago tal cual como los conocemos actualmente.

El cifrado como base de la seguridad de los datos transaccionales

A pesar de que muchas de las técnicas de obtención no autorizada de datos de tarjetas de pago descritas anteriormente radican en las vulnerabilidades inherentes a la tarjeta física de pago, otras (como la captura de tráfico y el almacenamiento inseguro de datos en memoria intermedia o medios persistentes) pueden ser controladas a través de técnicas criptográficas. Esto, en conjunto con controles adicionales de integridad para prevenir la manipulación no autorizada de los terminales de pago durante todo su ciclo de vida, ofrecen

una línea base de protección a las transacciones minimizando el riesgo de exposición de los comerciantes y de entidades intermedias (proveedores de servicios, bancos adquirientes, etc.) a potenciales accesos no autorizados a datos de pagos con tarjetas.

Para comprender la aplicabilidad de los controles de cifrado en este modelo, es importante conocer los pasos que se deben seguir en una transacción presencial en línea:

1. Los datos de la tarjeta son obtenidos a través de interacción física con el plástico, empleando la lectura de la banda magnética, la lectura del chip EMV o sin contacto (*contactless*) vía NFC.

2. Luego, los datos de autenticación (en este caso, el PIN) son solicitados al titular de la tarjeta, quien los digita empleando un teclado.

3. Ambos conjuntos de datos capturados (los datos de la tarjeta y los datos del PIN) son enviados al banco adquiriente.

4. El banco adquiriente envía estos datos al banco emisor para autenticar al titular y autorizar la transacción.

En función de los datos que se vayan a proteger (datos de la tarjeta (punto 1) o datos del PIN (punto 2)), el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago ("*Payment Card Industry Security Standards Council*" o PCI SSC, conformado por VISA, American Express, MasterCard, Discover y JCB), cuenta con dos estándares de seguridad asociados, que se analizarán a continuación:

- **Payment Card Industry (PCI) PIN Security (PCI PIN)**, para la protección del PIN, y
- **Payment Card Industry (PCI) Point-to-Point Encryption (PCI P2PE)**, para la protección de los datos de tarjeta.

PCI PIN: Protección del Número de Identificación Personal (PIN)

Los orígenes del estándar **Payment Card Industry (PCI) PIN Security (PCI PIN)** datan de 1995 con el programa "PIN Security & Key Management" de VISA. Dichas bases fueron adoptadas por el PCI SSC para el desarrollo de la primera versión del estándar en 2011. Posteriormente, en 2014 se publica la versión 2.0 y en 2019 se publica la versión 3.0[5]. Este estándar forma parte del grupo de estándares de seguridad de las transacciones con PIN denominado "PIN Transaction Security" (PTS), del cual también forman parte los siguientes estándares:

- PCI POI (Point-of-Interaction) para fabricantes de dispositivos de captura de datos como "Encrypting PIN pad" (EPP), "PIN entry device" (PED) y "Unattended payment terminal" (UPT), y
- PCI HSM (Hardware Security Module) para dispositivos de seguridad para la gestión de claves de encriptación.

El objetivo del estándar PCI PIN es la definición de un conjunto de requerimientos para la gestión segura, el procesamiento y la transmisión del número de identificación personal (PIN). Este estándar es aplicable a todas aquellas entidades involucradas en el procesamiento de transacciones *online* y *offline* con tarjetas de pago en cajeros electrónicos y terminales de punto de venta atendidas y desatendidas, incluyendo también a proveedores de dispositivos de pago y otros proveedores de servicios que puedan afectar a la seguridad del PIN (inyección de claves, gestión de dispositivos, entidades certificadoras, etc.).

En términos generales, PCI PIN define los siguientes lineamientos de seguridad:

- El PIN del titular de la tarjeta se debe capturar en dispositivos de seguridad homologados por el estándar PCI PTS POI. Esto garantiza que el dispositivo cuenta con controles específicos de encriptación, identificación de manipulación ("*tampering*") y seguridad física.
- El dato del PIN debe ser encriptado con criptografía robusta directamente en el dispositivo de captura. En este caso, tres esquemas criptográficos son soportados actualmente:

– **Fixed key**, en el cual se usa una clave criptográfica estática única por cada dispositivo para encriptar el PIN (este esquema será obsoleto a partir del primero de enero de 2023).

– **Master Key/Session Key (MK/SK)**, en el que la clave de encriptación del PIN es rotada periódicamente. Dicha clave es encriptada durante su transporte con una clave de encriptación de claves (Key-Encryption Key – KEK).

– **Derived unique key per transaction (DUKPT)**, en el cual se usa una clave de encriptación para el PIN única por cada transacción, derivada de una clave maestra (*Base Derivation Key* – BDK), conocida solo por la entidad adquiriente.

- Del lado de la entidad adquiriente (quien recibe la transacción), las claves de encriptación del PIN deben ser gestionadas empleando un módulo de seguridad de hardware (HSM) homologado por los estándares PCI HSM o FIPS 140-2 Level 3.
- Igualmente, dichas claves deben ser administradas de forma segura durante todo su ciclo de vida (generación, almacenamiento, distribución/transporte, carga, gestión de incidentes, retiro o remplazo y eliminación) siguiendo controles y procedimientos estrictos tanto en términos de seguridad física como de seguridad lógica.
- Se requiere la aplicación de controles de seguridad físicos y lógicos durante el ciclo de vida de los dispositivos de captura y gestión del PIN, desde su envío desde el fabricante hasta su despliegue en las ubicaciones del comerciante.
- Otros servicios especializados (como inyección remota de claves simétricas empleando criptografía asimétrica o servicios de inyección de claves) cuentan con requisitos de seguridad específicos.

Es importante anotar que el estándar PCI PIN es de obligatorio cumplimiento para todas aquellas entidades involucradas en la gestión del PIN.

Payment Card Industry (PCI) Point-to-Point Encryption (PCI P2PE): Protección punto a punto de los datos de tarjeta

En una transacción de pago tradicional, los datos de la tarjeta de pago ("*Account Data*") capturados mediante la lectura de la banda, del chip EMV o vía "*contactless*" se suelen enviar en texto claro desde el dispositivo de captura hasta el centro autorizador. Este procedimiento, claramente inseguro, sigue siendo empleado hoy en día por razones históricas y debido a ello es que han sucedido la mayoría de los incidentes de seguridad vinculados con acceso no autorizado a datos de tarjetas de pago.

La pregunta obvia en este punto sería: Ya que se emplea criptografía robusta para la protección del PIN (usando PCI PIN), ¿por qué no se usa un modelo similar para proteger todos los demás datos de la tarjeta de pago (principalmente el PAN)?

Precisamente aquí entra el estándar **Payment Card Industry (PCI) Point-to-Point Encryption (PCI P2PE)**. La primera versión de este estándar fue publicada en el año 2011, con una segunda versión en el año 2015 y una tercera versión (actual) en el año 2019[6].

Este estándar permite el cifrado de los datos de la tarjeta desde el punto de captura en el comercio ("*Point of Interaction*" – POI) hasta el proveedor de servicios, empleando criptografía robusta y protegiendo cualquier dato sensible en texto claro entre estos dos puntos (encriptación punto-a-punto). De esta manera, cualquier elemento intermedio en el flujo de la comunicación no podrá tener acceso a estos datos en claro, minimizando el riesgo y la necesidad de implementación de controles de seguridad adicionales.

Muchos de los controles de seguridad de PCI P2PE provienen de PCI PIN y siguen su misma línea, en donde lo único que cambia es el dato a proteger. No obstante, debido a que el estándar PCI P2PE protege al dato del PAN,

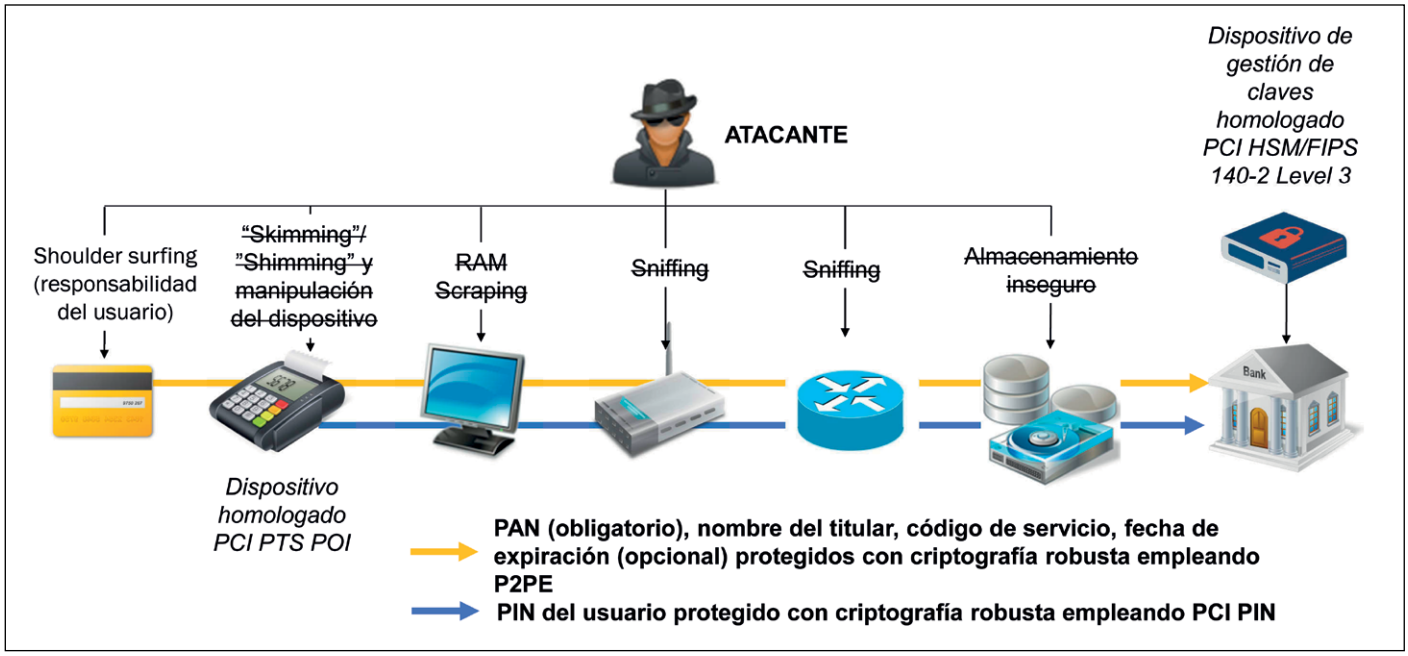

Figura 3.- Riesgos gestionados empleando controles de criptografía robusta provistos por PCI PIN (para el PIN) y PCI P2PE (para los datos de tarjeta).

tiene incidencia directa en el cumplimiento de otro estándar adicional: *PCI Data Security Standard* (PCI DSS). Aquellos comerciantes que hagan uso de este tipo de soluciones minimizan de forma importante el potencial riesgo de incidentes con datos de tarjetas, ya que no tendrán acceso a estos datos en claro posterior a su captura ni tendrán acceso a las claves de encriptación. Por esta razón, solamente requieren implementar un subconjunto de controles mínimo de PCI DSS en su entorno (SAQ P2PE) o incluso podrán quedar exentos de cumplimiento dependiendo de las políticas de cada marca[7-8].

Cabe anotar que el uso de una solución de pago homologada como P2PE[9] por parte de los comerciantes es opcional.

¿Por qué implementar PCI PIN y PCI P2PE?

Tal y como se ha descrito a lo largo de este artículo, los datos de tarjetas de pago son uno de los objetivos más deseados por los delincuentes. Para minimizar su potencial riesgo de exposición no solo en los comercios sino también en otras organizaciones involucradas en su gestión (bancos, proveedores de servicio, pasarelas de pago, etc.) se requiere el despliegue de controles de seguridad lógica y física específicos: PCI PIN para la protección del PIN (obligatorio para aquellas organizaciones que gestionan, procesan o transmiten este dato) y PCI P2PE (opcional, para la protección de los datos de la tarjeta). Mediante el uso complementario de estos dos estándares se puede obtener lo siguiente:

- Minimización del riesgo en la gestión del dato del PIN y de los datos de la tarjeta de pago del titular de tarjeta.
- Minimización del entorno de cumplimiento PCI DSS del lado del comerciante, con su correspondiente ahorro en costes, personal y tiempo.
- Control seguro de la transacción por parte del adquiriente y de entidades intermedias.
- Uso de estándares reconocidos por la industria.

Finalmente, este es un llamado a aquellos comerciantes, proveedores de servicios de pago y entidades financieras preocupados por la seguridad de los datos de tarjetas de sus clientes a que se documenten y definan acciones orientadas hacia la alineación de sus entornos con estándares reconocidos para la seguridad de estos datos, con el fin de minimizar potenciales riesgos y facilitar la adecuación de medidas específicas para la seguridad del ecosistema de pago. ■

David E. Acosta Rodríguez
Senior Security Consultant
CISSP, CISM, CISA, CRISC, CEH, CHFI
Qualified Security Assessor (QSA) for PCI DSS, PCI PIN, PCI P2PE, PCI 3DS and PCI TSP
ADVANTIO
david.acosta@advantio.com

REFERENCIAS

1 Diners Club International: The Story Behind the Card https://www.dinersclubus.com/home/about/dinersclub/story
2 Banco de España: Estadísticas sobre tarjetas de pago https://www.bde.es/f/webbde/SPA/sispago/ficheros/es/estadisticas.pdf
3 Diebold Nixdorf: ATM Security - Skimming vs. Shimming https://blog.dieboldnixdorf.com/atm-security-skimming-vs-shimming/
4 Square: The State of the U.S. EMV Migration - When Will Everyone Have Chip Cards? https://squareup.com/us/en/townsquare/the-state-of-the-u-s-emv-migration-when-will-everyone-have-chip-cards
5 Payment Card Industry (PCI) PIN Security - Requirements and Testing Procedures v3.0 https://www.pcisecuritystandards.org/documents/PCI_PIN_Security_Requirements_Testing_v3_Aug2018.pdf
6 Payment Card Industry (PCI) Point-to-Point Encryption – Security Requirements and Testing Procedures v3.0 https://www.pcisecuritystandards.org/documents/P2PE_v3.0_Standard.pdf
7 Mastercard Site Data Protection (SDP) Program - PCI DSS Validation Exemption Program for Eligible Merchants Using Secure Technologies https://globalrisk.mastercard.com/wp-content/uploads/2018/10/PCI-Validation-Exemption-Program.pdf
8 VISA: Small Merchant Security Program Requirements https://usa.visa.com/dam/VCOM/download/merchants/bulletin-small-merchant-security-faq.pdf
9 PCI Point-to-Point Encryption (P2PE) Solutions https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions