U.S. Payments Security Evolution and Strategic Road Map

Developed by the working groups of the Payment Security Taskforce

November 3, 2014

Contents

Introduction

The U.S. electronic payment card security landscape is changing more quickly than ever before due, in part, to new and emerging payment and security technologies as well as increasingly sophisticated fraud methods. In order to ensure that the industry successfully addresses the threats of today while anticipating the challenges and opportunities of the future, the U.S. Payments Security Task Force (PST) was assembled in early 2014. The task force is comprised of leading U.S. issuers, acquirers, merchants, payment networks and other electronic payment participants. Members of the PST have collaborated on this paper in order to detail payment card fraud threats and to offer recommendations to the various industry participants on how to navigate the challenges of today and the near future.

U.S. Payments Security Landscape

Payment Card Fraud and Underlying Risks

While much is being done to protect payment transactions and fraud is at historic lows, payment card data continues to be an attractive target for criminals who desire the financial opportunity of using or selling stolen payment card information. There are two primary types of payment card fraud that result from data breaches and the consequent compromise of account data.

- Counterfeit fraud occurs when sensitive account data from a magnetic stripe card is stolen. This data includes the primary account number (PAN), expiration date and a static card verification code. Because this code is static, as opposed to a dynamic or one-time-use code, it does not offer strong protection against fraud. Once a criminal obtains this information, he can use it to create a counterfeit payment card.
- Card-not-present (CNP) fraud occurs when the PAN and expiration date are stolen or otherwise compromised and then used for fraudulent transactions in remote-access payment channels, such as eCommerce, phone/mail orders or recurring payment situations. CNP fraud can result from the harvesting of PAN and expiration date from magnetic stripe or chip-read transactions or from remote-payment transactions such as eCommerce.

Both types of fraud can result from sensitive account and payment information being stolen using various methods. Data storage and processing systems across the payments ecosystem are necessarily large, complex systems that consist of a combination of internal networks, Internet-facing servers, software applications and remote-access capabilities for employees and third-party service providers. Such systems are designed with security in mind and require continual maintenance and updating. Criminals relentlessly seek to identify and exploit any vulnerabilities that may exist or arise within the system. Attack methods include use of malicious software (malware) to harvest cardholder data from inside these systems, and social engineering, or using insiders to gain access and control of systems in order to exfiltrate account data.

According to the 2014 Trustwave Global Security Report, electronic payment system attacks span a wide variety of merchant categories. The retail industry is the top category targeted by criminals, with 35% of the attacks. Food and beverage is second, with 18%, and hospitality is third, with 11%.

Many anti-fraud measures are currently in place. For example, merchants, acquirers, issuers and payment networks have invested in neural network models and complex business rule management systems designed to detect fraudulent transactions. Additionally, use of PIN encryption within the secure environment of payment terminals renders compromised PIN transaction data useless for criminals.

But ongoing security challenges indicate that additional measures and strategies for fraud protection and prevention are in order. While many current "best practices" center on securing system periphery with the intent of preventing breaches, the PST urges a focus on devaluing or eliminating sensitive data as it moves within and between systems. A multi-layered approach to security that includes compliance with PCI standards is called for, as no one solution alone is sufficient to combat payment card fraud. Three technologies that will play vital roles in this approach are chip technology, tokenization and encryption.

Chip Technology

Chip cards are payment cards that offer enhanced security over traditional magnetic stripe cards. In contrast to the static 3-digit verification code of mag stripe cards, chip cards use a dynamic authentication code that is generated

for each transaction. Chip technology has been used around the world for 20 years and is currently being implemented in the U.S.

As has been shown in markets outside the U.S., widespread adoption of chip technology helps to greatly reduce counterfeit fraud. This is because, in the event of a data breach, when the PAN, expiration date and dynamic authentication code are stolen, the authentication code of chip card cannot be replicated. Once a code has been used in a transaction, it will no longer be valid; therefore, a counterfeit card bearing the harvested PAN, expiration date and authentication code will not be authorized during a fraudulent transaction.

Chip technology will soon protect a large number of U.S. electronic payment transactions due to pending implementations by the largest merchants and aggressive issuer card replacement plans. According to chip migration forecasts from surveys compiled by the PST, issuers surveyed by the PST estimate that one in two U.S. credit and debit cards will be chip-enabled by the end of 2015. The PST reports that among acquirers that participated in the survey, 47% of terminals will be enabled to accept chip cards. This is a clear indicator that merchants are investing in technology to accept chip cards by the end of 2015. The size of the U.S. market, however, suggests that at least 3-5 years will be needed to reach full maturity of chip card acceptance.

In order to encourage accelerated adoption of chip technology in card issuance, terminals and ATMs, the largest U.S. payment networks have introduced liability shifts that will go into effect in October 2015 for point-of-sale terminals. Currently, issuers typically bear the liability for counterfeit fraud in card-present point of sale and ATM transactions. Once the liability shifts take place, if counterfeit fraud occurs on a contact chip-capable card and the merchant is not contact chip-card capable, the acquirer will be held liable for the transaction. Domestic and cross-border transactions will be included in the shift, while card-not-present transactions will not be included.

The liability shifts for individual brands may vary with respect to specific details. The objective of the liability shifts is to reward merchant, acquirer and issuer investments in chip technology, ultimately creating a more secure payments environment where chip-on-chip transactions occur.

While chip technology is designed to prevent counterfeit fraud, it is important to note that chip cards do not protect against theft of the PAN or expiration date, as data remains “in the clear” unless otherwise protected. As a result, theft of chip transaction details has the potential to result in

cross-channel fraud in remote transaction environments that require only the PAN and expiration date, such as some eCommerce and mail/phone orders. For this reason, additional technologies have been developed for further protection. Both tokenization and encryption provide for devaluing sensitive account data as it moves within and between systems.

Tokenization

Tokenization is the practice of replacing an account number with a substitute value. If this substitute value is stolen, the criminal's ability to use it for fraudulent transactions is limited.

The PST has categorized tokenization solutions into three broad types and is collaborating with industry standards bodies to establish alignment around these categories and associated terminology. This alignment, along with the development of educational materials that describe the nature and

scope of each solution type, can help increase industry awareness concerning tokenization that may enhance ongoing adoption efforts.

EMV Tokens

In March 2014, EMVCo released the first version of an industry-aligned tokenization specification that details a technical framework for securing digital payments.

The EMVCo specifications describe a token as a 13- to 19-digit number that substitutes for and has the appearance of the PAN. It is created by or on behalf of the issuer and provides protection from the time of payment initiation until de-tokenization (re-mapping from token back to PAN) in a secure token vault. Tokens may use dynamic cryptograms and carry domain controls limiting the payment environments in which a particular token can be used, and thus reduce fraud. A token is presented at the time of payment, though the cardholder may not realize a token is being used.

Deployment of tokens is under way, with initial use cases focused on mobile device payment enablement and card-on-file merchants. Solutions based on the EMVCo token specification offer the opportunity of eliminating the PAN and expiration date from merchant and acquirer environments and are designed to interoperate with existing acquiring tokenization solutions as well as chip cards. Efforts are also under way to develop interoperable payment account identifiers that preserve the ability of acquirers and processors to link transactions for loyalty and other value-added services while removing the need for PAN. Broad market adoption of tokenization will likely take several years.

Acquiring Tokens

Acquiring tokens have been in use for about 10 years as substitutes for PAN, expiration date and other sensitive account data within the closed environment between the acquirer and merchant, within a merchant environment, or within a service provider environment. Acquiring tokens are created after the cardholder presents payment credentials. They allow for the removal of sensitive account data during storage and may also protect data in transit within this section of the transaction stream. Acquiring tokens are also frequently used in card-not-present transactions, such as eCommerce, and are typically coupled with encryption. Some acquiring tokens are used for payment transaction initiation, however in all cases acquiring tokens are converted back to the original PAN before being sent outside the closed environment for which they are intended. Acquiring tokenization solutions

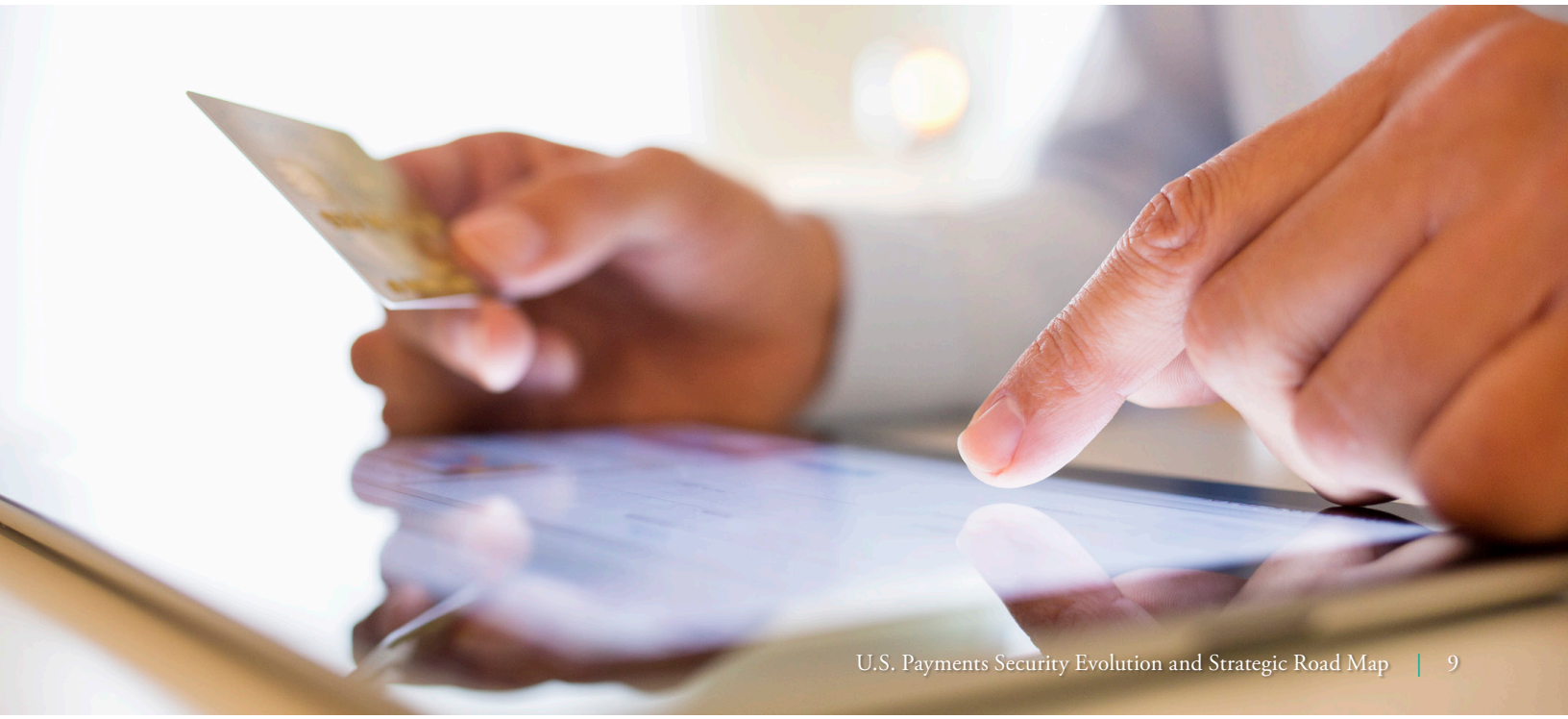
are proprietary and are not based on an industry standard approach to token generation, format, request or provisioning. Although various standardization efforts are under way, there are currently no standards in place that provide guidance in aligning acquiring tokens with other types of tokens to ensure interoperability and reduce implementation and operational problems.

Issuer Tokens

Issuer tokens, also known as virtual card numbers, are created by issuers and provide the means to reduce risk in specific use cases, including commercial card applications, as well as consumer-oriented services. These tokens resemble the PAN, so merchants and acquirers are unlikely to know that they are using a token.

Point-to-Point Encryption

Point-to-Point Encryption is the process encrypting payment data in a secure terminal and transmitting it through an internal or external network where it is decrypted in a secure environment. Point-to-Point Encryption is currently in use in the U.S. payment card industry and can be used alone or with acquiring tokenization and chip. Industry standards, such as the PCI Data Security Standard, call for encryption to protect data at rest and



any time card data is transmitted over a public network, but encryption can also be initiated at the beginning of a transaction to protect data from being compromised inside of a merchant environment by malware or other means. Encryption solutions are widely available in the U.S. but only moderately adopted.

Many current-generation terminals include a capability to initiate encryption of payment data securely within the terminal itself after the card has been read for either a magnetic stripe or chip transaction. Encryption that occurs within the terminal itself is more secure than encryption that is effected outside of the terminal and farther downstream in payment processing because the latter method leaves PAN and other sensitive data in the clear and, thus, vulnerable to threats such as malware until encryption occurs.

Like acquiring tokenization, point-to-point encryption solutions are mostly proprietary in nature. The PCI Security Standards Council's voluntary Point-to-Point Encryption Program addresses the security of the encryption process, but has not been widely adopted. The PCI SSC is partnering with industry stakeholders to optimize the program and promote broader industry support.

Other Technology Considerations

Technologies used to authenticate cardholders in remote-payment environments like eCommerce can also serve to combat card-not-present fraud. Authentication services are generally based on the 3-D Secure protocol and include MasterCard SecureCode Plus, Verified by Visa, American Express SafeKey and JCB's J/Secure. These have historically been more widely adopted outside of the U.S., but increased activity is now being realized within the U.S. These authentication solutions are designed to secure browser-based online purchases and to support the trend toward in-app payments.

In addition to authentication technologies, merchants, acquirers, processors, payment service providers, issuers and payment networks have deployed fraud screening and detection tools that incorporate device ID and risk-based decisioning engines to screen CNP transactions for fraud.

Future Landscape

The future landscape of electronic payments in the U.S. will look much different than the current one. Electronic payments are evolving in ways that blur the line between transaction methods at brick-and-mortar retailers and those with online merchants. Mobile devices are fueling payment and customer experience innovation and are expected to lead to a progressive

convergence between the physical and digital worlds. This convergence likely will alter how consumers shop at physical and virtual merchant locations, as payment methods transition from traditional plastic cards to digital payments. It is imperative that security innovation keeps pace with the continuously evolving convergence of consumer buying experiences.

While chip technology will continue to be a cornerstone for payment security to ensure that counterfeiting risks are contained, payment technologies are evolving beyond traditional card-based payments to include secure elements inside of mobile devices or within "the cloud." As the market progresses toward secure payment technologies such as contact and contactless chip, magnetic stripe transactions will shrink to a small percentage of overall transaction volume.

As long as magnetic stripe data is being stored or processed, the industry will need to continue to protect that data to reduce the risks of compromise and subsequent counterfeit fraud. As the transaction mix becomes more digital in nature, however, elimination of PAN and sensitive data will become achievable.

As chip penetration increases in the U.S., the role of authentication will also increase as more industry focus is concentrated on reducing CNP fraud. Existing frameworks for 3-D Secure will be enhanced to offer more robust and dynamic forms of authentication. Current protocol specifications will likely evolve toward device ID collection and communication. Similarly, these specifications could evolve to support authentication of in-app purchases and the identification and verification frameworks for tokens.

Security Priorities

Now is the time for all stakeholders to aggressively push for near-term adoption of secure chip technologies in the U.S. This commitment is vital to protect against counterfeit fraud and ensure ongoing interoperability with global cardholders and merchants that have already fully transitioned to chip. This investment will pay near-term and future dividends for all U.S. electronic payments industry participants, because chip adoption paves the way to a more secure payments landscape.

As merchants move forward with deployment of chip acceptance solutions, they should also evaluate the enablement of contactless acceptance capabilities. Doing so will enable merchants to transact with a growing base of contactless-enabled cards as well as mobile devices enabled for secure contactless payments.

Recognizing that the current U.S. payments landscape includes vulnerabilities that can result in the theft of sensitive data and consequent fraud—even as the U.S. moves to chip technology—it is imperative that key industry stakeholders demonstrate leadership by acting now to implement additional layers of security. These include data protection mechanisms, such as encryption and acquiring tokenization, as well as the elimination of sensitive data through broader emerging solutions based on payment network tokens.

Data protection and data elimination solutions can coexist and interoperate for years to come and are compatible with existing security and business frameworks as well as future device-based payment solutions. The pace of change should only be expected to accelerate, and therefore, as acquirers and merchants consider alternative designs, consideration should be given to less-integrated structures that may be nimbler and easier to upgrade and adapt in the future.

Key Recommendations by Stakeholder

Following are the PST's recommendations for Chip, Encryption and Tokenization by key payments industry stakeholders.

Merchants

Merchants play an important role in the security of card payments, and therefore, key recommendations for the merchant community are:

CHIP

- Understand the potential impact of each payment brand's liability shift programs.
- Planning, purchase, deployment, integration, certification and implementation can take months, so ensure that chip terminal upgrades are planned for well in advance of the liability shift.
- Merchants should plan to educate store personnel about terminal migration and operational changes.
- When upgrading terminals for chip, consider the capabilities of the terminal to support hardware-based encryption and contactless/NFC payments.
- Merchants can readily take advantage of multiple debit network routing options by deploying the common debit AID, which was developed through industry collaboration to ensure merchant routing choice for U.S. EMV chip debit transactions.

TOKENIZATION

- Merchants currently storing PANs should consider migrating to tokenization solutions to reduce the underlying risks and fraud impact of a data compromise.
- Consider deploying/developing solutions to reduce the reliance on PAN for value-added services. Solutions may include the development of interoperable payment account identifiers that preserve the ability of acquirers and processors to link transactions for loyalty and other value-added services while removing the need for the PAN.

ENCRYPTION

- Consider adopting hardware-based encryption using a full PCI PTS and Secure Read & Exchange of Data (SRED)-approved terminal. Although the industry may benefit over time from further standardization of encryption, merchants should not defer implementation of an encryption solution, since existing solutions can reduce risk.
- Consider avoiding solutions that only encrypt outside of the terminal, since such solutions leave sensitive data vulnerable for a longer period of time and, therefore, are less secure than those that encrypt inside the terminal.
- Consider implementing encryption solutions that decrypt transactions outside of the merchant's own environment. Decryption should only be performed within a trusted and secure third-party platform managed by an acquirer, processor or other trusted party with the security know-how and resources to ensure a secure decryption environment and secure management of encryption keys.

While breach insurance may be of some value to the merchant community, it is crucial to understand that it is not sufficient protection from the reputational and financial impact of a data breach. Breach insurance should not be considered an alternative to adoption of chip, encryption, tokenization or other layers of security.

In addition, merchants should consider increasing their involvement in the development of new payment standards by participating in industry standard bodies such as the PCI Security Standards Council through their Participating Organization program and EMVCo through their Associate Program (EAP) to provide input into the standards creation process for existing and emerging payments technologies.

Acquirers/Processors

It is recommended that acquirers and acquirer processors adopt the necessary technology to enable them to continue to process a wide variety of transactions, including those initiated from consumer mobile devices. Specific recommendations are:

CHIP

- If not already completed, certify for chip transactions with payment brand networks (April 2013 mandates).
- Understand the potential impact of the payment brands' liability shift programs and communicate the potential impacts to merchants.
- Consider prioritizing highest-risk merchant categories (retail, food and beverage, hospitality) and ensure all merchants' understanding and support of chip adoption, both contact and contactless.
- Consider making operational updates with regard to the liability shifts, such as changes to chargeback processing, and communicate these operational changes to merchants with ample lead time prior to the liability shift date.

- Consider helping merchants determine how far in advance they will need to initiate projects for chip enablement to meet their intended launch dates.
- Consider how to streamline chip certification processes and educate merchants, independent sales organizations (ISOs) and value-added resellers (VARs). Consider leveraging network self-certification programs as part of this effort.

TOKENIZATION

- Consider supporting a full range of tokenization solutions, including acquiring tokens that can be deployed along with encryption services, to fully protect sensitive data, whether at rest or in transit. Consider implementing payment network transaction message support for tokens to ensure interoperability among the different types of tokens.
- Consider developing strategies for eliminating dependence on the PAN in back office and transaction lifecycle functions. Consider participating in industry efforts to look at alternatives to using the PAN in the acquiring ecosystem.

ENCRYPTION

- Consider partnering with technology vendors and offering merchants encryption solutions that facilitate the ongoing protection of PAN and other sensitive data.

Issuers

Issuers also face a variety of important decisions and key investments in security. Recommendations for issuers are:

CHIP

- Consider deploying chip cards now, or as early as possible, keeping in mind the payment brands' liability shift programs as well as the goal of reducing the number and value of magnetic stripe transactions and the threat of counterfeit fraud. Debit issuers should contact their unaffiliated network and/or processor to determine their readiness.
- Consider discussing chip migration plans with your processors and networks. There are a number of options available to issuers in the configuration of cards, and it is vital to begin migration planning early. Most processors and networks have experts and tools available to assist in navigating these decisions.
- Consider playing a primary role in consumer communication concerning the introduction and use of chip cards.

- Consider continued deployment of a layered security approach that integrates chip while maintaining and fine-tuning existing fraud detection and monitoring services.
- Consider continuing to optimize fraud services to address residual magnetic stripe fraud risks, magnetic stripe fallback (when the terminal does not communicate with the chip) and fraud migration to card-not-present channels.

TOKENIZATION

- Consider putting in place product strategies to capitalize on the changing landscape of payments, including capabilities to enable consumer mobile devices for payment. This includes support for tokens in order to drive strategies that begin to eliminate PAN and other sensitive data from the payments ecosystem.
- Consider promoting and participating in industry efforts focused on eliminating the use of PAN for value-added services outside of the

issuer itself. Solutions may include the development of interoperable payment account identifiers that preserve the ability of acquirers and processors to link transactions for loyalty and other value-added services while removing the need for PAN.

- Upon the introduction of payment account identifiers, consider the underlying business and security value in placing tokens on chip cards to further drive the elimination of PAN in the payments ecosystem.

Payment Systems

The changing landscape of electronic payments and evolving security frameworks impacts payment systems. Recommendations for this stakeholder community are:

CHIP

- Continue efforts to reduce friction associated with the implementation of chip and learn from other markets that have achieved a mature state of adoption of chip cards and terminals.
- Consider sharing best practices for key adoption and implementation hurdles, including acquirer, system integrator and VAR certification.

TOKENIZATION

- Consider publishing and sharing best practices for coexistence of chip with all forms of tokenization.
- In conjunction with industry stakeholders, consider developing payment account identifiers to ensure that existing merchant and acquirer systems continue to be efficient when operating with tokens, and consider working with EMVCo to update the standards accordingly.
- Consider communicating options to perform token vault and other token service provider functions within the EMVCo specification.
- Endeavor to ensure that the evolution of EMVCo tokenization meets the ongoing needs of payment system stakeholders, including acquirers, issuers, processors, cardholders and merchants, and satisfies regulatory requirements. Consider communicating the role of tokenization in securing or eliminating sensitive data throughout the traditional merchant landscape as well as emerging omni-merchant deployments.

ENCRYPTION

- Consider publishing and sharing best practices for coexistence of chip with encryption.

- Consider identifying best practices for deploying software-based encryption solutions in environments in which traditional hardware-based encryption solutions are not available.

Integrators and Value-Added Resellers (VARs)

System integrators and VARs are engaged in the implementation and ongoing development of merchant payments infrastructure in the U.S., including integration and coexistence with other point-of-sale platforms. Recommendations for integrators and VARs are:

- Ensure that all new terminals contain, at a minimum, chip capability in hardware. Additionally, consider implementing support for contactless/NFC acceptance.
- Consider developing integration strategies and architectures that appropriately weigh the impact of security upgrades and ongoing maintenance for technologies, including chip, tokenization and encryption, as part of the initial design to reduce the friction when upgrades are desired or necessary.
- Consider token integration as part of the overall implementation of payments to reduce the exposure of sensitive data in non-payment systems that are subject to compromise.
- Consider seeking guidance from the standards bodies on how all three categories of tokens should work together. Appropriate standards can help integrators deploy solutions more efficiently, as many will find their payment solutions integrating with dozens of acquirers and gateways.

References

EMVCo Specifications:
http://www.emvco.com

PCI Security Standards Council:
https://www.pcisecuritystandards.org/

Trustwave Global Security Report:
https://www.trustwave.com/gsr

Glossary

Acquiring token—A token created by the acquirer, merchant or a merchant's service provider. This token is created after the cardholder presents their payment credentials. Acquiring tokens may be used as part of the authorization process, including card-on-file transactions.

Cloud computing—Internet-based computing that utilizes a shared pool of resources (e.g., networks, servers, storage, applications and services) to manage, store and process data.

Card-not-present transaction—A transaction that does not require a physical card to be present at the time of purchase, such as for eCommerce, mail or telephone orders.

Card-not-present fraud—The use of stolen or compromised PAN and expiration date data to conduct fraudulent transactions in remote payment channels such as eCommerce, mail order, telephone order and recurring payments.

Card-present transaction—A transaction that requires a card to be present at the time of the transaction.

Contactless—Contactless smart chip technology that relies on a secure microcontroller or equivalent intelligence, internal memory and a small antenna embedded in a device that communicates with a reader through a contactless radio frequency (RF) interface.

Counterfeit fraud—The creation of unauthorized magnetic stripe cards that use stolen data and that generally include the full content of the magnetic stripe of compromised accounts.

Cryptogram—An alphanumeric value that is the result of data elements entered into an algorithm and then encrypted, commonly used to validate data integrity. The creation and validation of the cryptogram enables dynamic authentication. (Source: *EMV Migration Forum*)

Data protection—Solutions such as encryption and acquiring tokenization that help to protect sensitive account data in the merchant and acquiring domains.

De-tokenization—De-tokenization is the process of redeeming a Payment Token for its associated PAN value based on the Payment Token to PAN mapping stored in the Token Vault. The ability to retrieve a PAN in

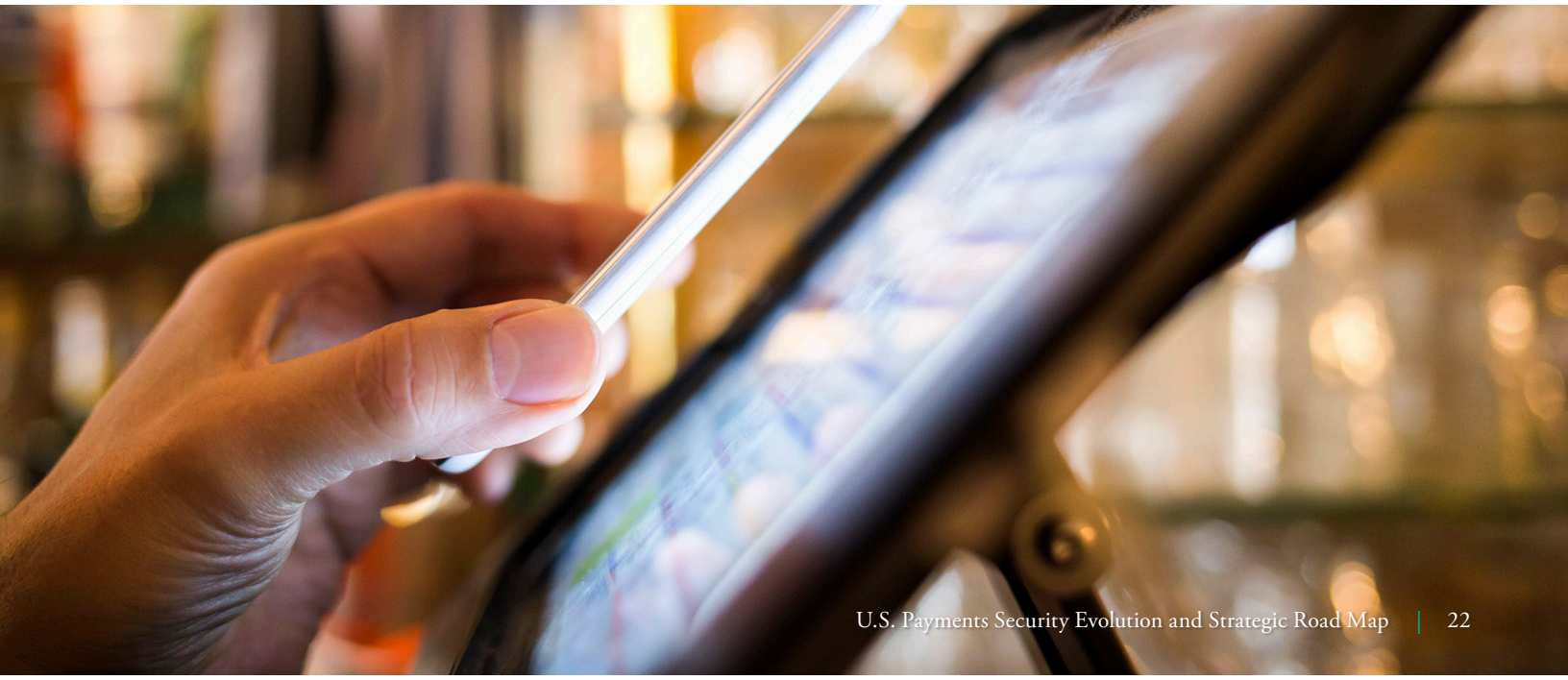
exchange for its associated Payment Token should be restricted to specifically authorized entities, individuals, applications, or systems. (Source: *EMVCo*)

Dynamic authentication data—Information that is used during a transaction to generate the cryptogram used to verify the card participating in the transaction and that changes from transaction to transaction. (Source: *EMV Migration Forum*)

EMV Chip—Specifications developed by Europay, MasterCard and Visa that define a set of requirements to ensure interoperability between payment chip cards and terminals. (Source: *EMV Migration Forum*)

EMVCo—The organization formed in February 1999 by Europay International, MasterCard International and Visa International to manage, maintain and enhance the EMV Integrated Circuit Card Specifications of Payment Systems. EMVCo is currently owned by American Express, Discover Financial Services, JCB, MasterCard Worldwide, UnionPay and Visa Inc. (Source: *EMV Migration Forum*)

Encryption/Decryption—Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized



disclosure. (Source: *PCI Data Security Standard: Glossary, Abbreviations and Acronyms*)

Fallback—The term used for the scenario when a transaction is initiated between a chip card and a chip terminal but chip technology is not used and the transaction is completed via magnetic stripe or key entry. (Source: *EMV Migration Forum*)

Hosted payment page—A merchant's Web-based payment page that is hosted by a third-party service provider that collects cardholder data and authorizes the transaction.

Integrated terminal/integrated point of sale (IPOS)— Terminals that are more sophisticated than traditional terminals in that they may be set up to communicate with other terminals owned by the same merchant—even if they are located at different locations. These systems handle both internal functions like inventory control as well as external ones (i.e., electronic funds transfer) and typically combine an electronic cash register with a card reader and a PIN keypad.

Integrator—An entity that sells and/or integrates payment applications but does not develop them. Also known as reseller. (Source: *PCI Data Security Standard: Glossary, Abbreviations and Acronyms*)

ISOs (Independent sales organizations)—Third-party organizations that partner with acquiring banks to find, open and manage merchant accounts on behalf of such businesses. (Source: *EMV Migration Forum*)

Issuer token—Tokens that are created by an issuer and resemble a PAN. Also known as virtual card numbers.

Liability shift program—A program that, in general terms, apportions fraud loss to the party to the transaction that has not invested in chip technology.

Lost/stolen fraud—Fraud that arises when a card is lost or stolen and a person who is not an authorized user of the card uses it to make fraudulent transactions.

Malware—Malicious software. Designed to infiltrate or damage a computer system, without the owner's knowledge or consent. (Source: *PCI Data Security Standard: Glossary, Abbreviations and Acronyms*)

NFC (Near field communication)—A standards-based wireless communication technology that allows data to be exchanged two-ways

between devices that are a few centimeters apart. NFC-enabled mobile phones incorporate smart chips (called secure elements) that allow the phones to securely store the payment application and consumer account information and to use the information as a "virtual payment card." NFC is an extension of Radio Frequency Identification (RFID). (Source: *EMV Migration Forum*)

PCI Data Security Standard (PCI DSS)—A framework developed by the PCI Security Standards Council (SSC) for developing a robust payment card data security process—including prevention, detection, and appropriate reaction to security incidents. (Source: *PCI SSC website:* www.pcisecuritystandards.org)

PCI Security Standards Council (PCI SSC)—The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements. (Source: *PCI SSC website:* www.pcisecuritystandards.org)

PIN (Personal identification number)—A numeric code of 4 to 12 digits that is used to identify cardholders at a customer-activated PIN pad. PINs can be verified online by the issuer or sent to the chip card for offline PIN verification. (Source: *EMV Migration Forum*)
Online PIN: In a chip transaction, the process of comparing the cardholder's entered PIN with the PIN stored on the issuer host system. The PIN is encrypted by the terminal PIN pad before being passed to the acquirer system. The PIN is then decrypted and re-encrypted as it passes between each party on its way to the issuer. This is supported today with mag-stripe.
Offline PIN: The PIN is stored on the chip card (versus a PIN stored at the host). In a chip transaction using offline PIN, the PIN entered at the terminal is compared with the PIN stored securely on the chip card without going online to the issuer host for the comparison. Only the result of the comparison is passed to the issuer host system. Two types of offline PIN are enciphered and plaintext.

PST (Payments Security Task Force)—The Payments Security Task Force was announced in March 2014 to drive executive-level discussion that will enhance payments system security. The task force is comprised of a diverse group of participants in the U.S. electronic payments industry, including payment networks, issuers, acquirers, retailers, point-of-sale device manufacturers and industry trade groups.

PTS (PIN transaction security)—PTS is a set of modular evaluation requirements managed by PCI Security Standards Council, for PIN acceptance POI terminals ("Point of Interaction," the initial point where data is read from a card). (Source: *PCI Data Security Standard: Glossary, Abbreviations and Acronyms*)

Remote transaction—Alternative term for a card-not-present (CNP) transaction.

SRED (Secure Read and Exchange of Data)—A modular set of security requirements that are a subset of the PCI PIN transaction security program and apply to a Point of Interaction (POI). A POI validated by a lab as meeting SRED requirements ensures that account data is protected at the point of acceptance by providing secure encryption methods, key management

and tamper protection which will assist in meeting the required security considerations of the wider point-to-point security process.

Sensitive authentication data—Security-related information (including but not limited to card validation codes/values, full track data, PINs and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

Static Data Authentication (SDA)—A card authentication technique used in offline chip transactions that uses signed static data elements. With SDA, the data used for authentication is static—the same data is used at the start of every transaction. This prevents modification of data, but does not prevent the data in an offline transaction from being replicated. (Source: *EMV Migration Forum*)

Tokenization—Tokenization is a process by which the PAN is replaced with a surrogate value called a token. Tokenization may be undertaken to enhance transaction efficiency, improve transaction security, increase service transparency, or to provide a method for third-party enablement. (Source: *EMVCo*)

Token vault—A repository, that maintains the established payment token to PAN mapping. The token vault may also maintain other attributes of the token requestor that are determined at the time of registration and that may be used by the token service provider to apply domain restrictions or other controls during transaction processing. (Source: EMVCo)

VARs (Value-added resellers)—Value-added resellers (VARs) are companies that add features or services to an existing product, then resell it (usually to end users) as an integrated product or complete "turn-key" solution.

Virtual card numbers—Virtual credit cards, also known as "single use" or "disposable" cards, offer a randomly generated substitute account number (issuer token) in place of the payment card number.

3-D Secure—Protocol designed to be an additional security layer for eCommerce transactions.

About the Payments Security Task Force

The Payments Security Task Force was announced in March 2014 to drive executive-level discussion that will enhance payments system security. The task force includes a diverse group of participants in the U.S. electronic payments industry including payment networks, banks of various sizes, credit unions, acquirers, retailers, point-of-sale device manufacturers and industry trade groups.

Among the participants are American Express, Bank of America, Capital One, Chase, Citi, Credit Union National Association, Discover, First Data, Global Payments Inc., Independent Community Bankers of America, Kroger, National Association of Federal Credit Unions, Marriott, MasterCard, Navy Federal Credit Union, Sheetz, Shell, Subway, US Bank, Vantiv, VeriFone, Visa Inc., Walgreens, and Wells Fargo & Company.