



COMMONWEALTH of VIRGINIA

Department of the Treasury

MANJU S. GANERIWALA
TREASURER OF VIRGINIA

P.O. BOX 1879
RICHMOND, VIRGINIA 23218-1879
(804) 225-2142
FAX (804) 225-3187

October 1, 2015

MEMORANDUM

TO: The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable Karen R. Jackson
Secretary of Technology

FROM: Manju S. Ganeriwala *Manju Ganeriwala*

SUBJECT: Department of the Treasury's Report -A Plan for Securing Consumer Transactions, as Required by Executive Directive 5

The Department of the Treasury is pleased to present to you "A Plan for Securing Consumer Transactions" as requested by Executive Directive 5 on May 5, 2015. This directive instructs Commonwealth agencies like the Department of the Treasury to adopt the latest security technologies in order to provide the highest levels of security possible for the Commonwealth's financial transactions. The attached document includes an executive summary of the report, the report itself, as well as appendices and a glossary explaining the finer details of the technology and processes involved in implementing this plan.

By enacting this plan, consumers doing business with the Commonwealth will enjoy the highest available industry standards for processing electronic financial transactions. Instances of fraud and breaches of electronic security systems should be significantly reduced under this plan, and the extent of and potential damage of such acts should be greatly mitigated. We look forward to working with you and all Commonwealth agencies to have this plan enacted in a swift and timely fashion.

Please do not hesitate to contact me should you have any questions or need additional information.

cc: The Honorable Paul J. Reagan, Chief of Staff to the Governor
The Honorable Richard D. Brown, Secretary of Finance

Department of the Treasury

A Plan for Securing Consumer Transactions

October 1, 2015

Executive Summary

On May 5, 2015, Governor McAuliffe issued Executive Directive 5 to ensure consumer financial data is properly secured by the Commonwealth of Virginia. Executive Directive 5 instructs Commonwealth agencies to adopt the latest security technologies in order to provide the highest levels of security possible for the Commonwealth's financial transactions.

The Directive required the Department of the Treasury to submit a plan on October 1, 2015, detailing efforts to enhance the security features of merchant and prepaid card programs in the following areas:

- User authentication
- Confidentiality
- Cardholder reporting of unauthorized withdrawals or fraudulent transactions
- Data breach reporting

The Department of Treasury possesses two key responsibilities when helping process financial transactions throughout many agencies in the Commonwealth. The first responsibility is to securely receive electronic payments. In this role, the Treasury, on behalf of state agencies that provide goods and services, works with its merchant card processing vendor to receive payments made through credit and debit card transactions. For example, the Treasury and its vendor assist the Department of Motor Vehicles (DMV) in helping process transactions when customers use their credit or debit cards to pay for services. The second responsibility is to help Commonwealth agencies make electronic payments to citizens. For example, the Commonwealth has adopted a prepaid debit card program to facilitate electronic disbursements when an individual has opted not to receive an automated bank account deposit, such as for unemployment benefits. Treasury is responsible for procuring statewide contracts for both the merchant card processor and the prepaid debit card vendor to help receive payments and make disbursements.

Treasury's plan meets the goals of Executive Directive 5 by adopting "EMV" encryption technology for both merchant card transactions and the issuance of prepaid debit cards. EMV is an acronym derived from the initials of the co-developers: Europay, MasterCard, and Visa. By adopting EMV standards, the Commonwealth will address the user authentication and confidentiality issues that have historically existed with magnetic strip cards. EMV does this by using a "smart chip" instead of a magnetic strip to hold cardholder information. Each time an EMV card is used, the chip creates a unique transaction code. That transaction code can only be used one time, thereby rendering the transaction code useless for potential fraudsters. Because of

this, adopting EMV technology will reduce fraud-related liability among our agencies and minimize having to report data breaches.

Treasury's contract with its merchant card process and prepaid debit card vendors already addresses Executive Directive 5's mandate to better report unauthorized withdrawals and data breaches. In addition, the adoption of EMV will reduce instances of fraud, meaning that fraud-related liability will be reduced, and there will be fewer data breaches that need to be reported.

The Commonwealth has made steady progress in adopting EMV for merchant transactions. As of October 1, 2015, 80 percent of all Commonwealth terminals had been converted to EMV technology. Since April 2014, all new terminals purchased and installed have been EMV-capable. Treasury is in the process of selecting a new prepaid debit card vendor to speed the conversion to EMV-capable prepaid debit cards.

Executive Directive 5 creates additional incentives for agencies to move forward in a timely manner to adopt more secure payment technologies. All processing terminals should be EMV capable by March 31, 2016 and all prepaid debit cards should be converted to chip embedded cards by December 31, 2016. These actions should provide the Commonwealth with the highest available industry standards for securing data.

Department of the Treasury

A Plan for Securing Consumer Transactions

October 1, 2015

Background

On May 5, 2015, Governor McAuliffe issued Executive Directive 5 to ensure consumer financial data is properly secured by the Commonwealth of Virginia. Executive Directive 5 instructs Commonwealth agencies to adopt the latest security technologies in order to provide the highest levels of security possible for the Commonwealth's financial transactions. The Department of the Treasury's plan responding to Directive 5 is presented in this document.

The Directive required the Department of the Treasury to submit a plan on October 1, 2015, detailing efforts to enhance the security features of merchant and prepaid card programs in the following areas:

- User authentication
- Confidentiality
- Cardholder reporting of unauthorized withdrawals or fraudulent transactions
- Data breach reporting

The Department of Treasury possesses two key responsibilities when helping process financial transactions throughout many agencies in the Commonwealth. The first responsibility is to securely receive electronic payments. In this role, the Treasury, on behalf of state agencies that provide goods and services, works with its merchant card processing vendor to receive payments made through credit and debit card transactions. For example, the Treasury and its vendor assist the Department of Motor Vehicles (DMV) in helping process transactions when customers use their credit or debit cards to pay for services. The second responsibility is to help Commonwealth agencies make electronic payments to citizens. For example, the Commonwealth has adopted a prepaid debit card program to facilitate electronic disbursements when an individual has opted not to receive an automated bank account deposit, such as for unemployment benefits. Treasury is responsible for procuring statewide contracts for both the merchant card processor and the prepaid debit card vendor to help receive payments and make disbursements.

Europay, Mastercard, and Visa (EMV) Technology

Treasury's plan calls for adopting "EMV" encryption technology for both merchant card transactions and the issuance of prepaid debit cards. EMV is an acronym derived from the initials of the co-developers: Europay, MasterCard and Visa. EMV provides a more secure transaction by using a "smart chip" instead of a magnetic strip to hold cardholder information.

Please see Appendix A for an illustration of how transactions using EMV technology are processed.

With traditional “swipe” payment cards, a cardholder swipes the payment card in the merchant’s card reader, transmitting the cardholder’s information (name, card number, expiration date, etc). EMV technology instead embeds EMV cards with a “smart chip.” Each time an EMV card is used, the chip creates a unique transaction code. That transaction code can only be used one time, thereby rendering the transaction code useless for fraudsters. If a fraudster steals the one-time transaction code from a specific point-of-sale device, the card will be denied on a future transaction since the code has already been used. The new code is embedded in the chip, minimizing the ability to create usable counterfeit cards. As a result, EMV cards provide a much greater level of user authentication and confidentiality.

The United States has been relatively slow to adopt EMV technology. Countries in Europe and other nations around the world have widely used EMV technology for years. With the growing concern for payment card fraud, the U.S. payment card industry has decided to adopt EMV technology with a target date of October 1, 2015.¹

This change in industry standard encourages merchants to obtain so-called ‘EMV readers.’ These readers allow a consumer to “dip” a card into the terminal, which then allows the reader to obtain the necessary information off of the EMV chip. Traditional swipe readers can still be used after this date; however, these readers will only be able to obtain the traditional magnetic strip data and not the chip’s unique transaction code. This change in best practices should encourage issuers of payment cards to provide cardholders with the new EMV “smart chip” cards in short order.

On October 1, 2015, entities with the weakest security measures will assume liability for any loss due to fraudulent activity. For example, if a merchant such as the DMV does not employ an EMV reader and a fraudster creates a counterfeit magnetic strip payment card, DMV would be liable for any fraudulent transactions since DMV did not adopt the newer technology. On the opposite side, if a merchant such as the DMV does in fact employ an EMV reader, and a fraudster makes a fraudulent transaction with a counterfeit magnetic strip payment card, then the issuer would have to assume the loss of that fraud. This change should encourage issuers and merchants to fully adopt EMV technology and thus make these transactions more secure.

The Commonwealth as a Merchant

Since the early 2000’s, the Commonwealth has accepted credit and debit cards for the payment of agency services such as licenses, fees, products, documents and other transactions. In this role, agencies accept payments like any merchant accepting credit cards. Treasury serves as the coordinator and procurer of card processing services for the agencies and also serves as the administrator for the optional, cooperative contract under which agencies and local governments

¹ See: *Wall Street Journal* “October 2015: The End of Swipe-and-Sign Credit Card” published February 6, 2014 by Tom Gara.

use the card processor. Currently, the provider of card processing services on behalf of Treasury is a company called Elavon.

In Fiscal Year 2015, the Commonwealth processed over 26 million credit and debit card transactions, totaling \$1.4 billion in revenue. This is an increase over Fiscal Year 2011's volumes of 18 million transactions and \$1.1 billion in revenue, representing a 44 percent and 27 percent increase respectively from FY 2011 to FY 2015. There are now nearly 1,600 agency locations supported under the processing card services contract.

In its lead role in facilitating card-based transactions for agencies, Treasury is working with the individual agencies and card processors to convert Commonwealth agency card readers (i.e. terminals) to accept EMV enabled cards. This requires newly designed terminals to encrypt the embedded transaction code for transmission to the processor. EMV terminals deployed by the Commonwealth employ a sophisticated "Triple DES" (data encryption standards) encryption when executing a payment. This means that the chip's authentication, transaction code, and message are all securely transmitted at the point of sale.

By fully adopting EMV technology, Treasury will meet the highest industry standards of card payment security available. As of October 1, 2015, 80 percent of all Commonwealth terminals have been converted to EMV technology. Since April 2014, all new terminals purchased and installed have been EMV capable. The two largest user agencies in terms of retail locations—the Department of Alcoholic Beverage Control (ABC) and the DMV—account for 35 percent of all terminals. Both agencies have integrated point-of-sale systems, meaning that these systems are directly linked (integrated) to the agency's financial network, and transactions are processed in this closed system.

These integrated systems have terminals that utilize EMV, as well as an additional layer of protection by using tokenization. *Please see Appendix B for a description and flow chart illustrating the tokenization process.* Tokenization takes card data and converts it into a random generated value that replaces sensitive information, such as a card number. It then passes on the randomized information to complete the transaction. This tokenization process adds another layer of protection when storing data, and only occurs at outlets with integrated terminals such as ABC and DMV. All ABC merchant outlets have EMV capable readers, as well as the extra encryption and tokenization. DMV merchant outlets are in the process of achieving this goal and plan to migrate all locations prior to the end of calendar year 2015.

Treasury is working with the remaining agencies to complete their conversion to EMV enabled terminals that do not require integrated point-of-sale systems. *Please see Appendix C for details of these conversion activities.* Treasury anticipates that Commonwealth credit and debit card terminals will be EMV capable by March 31, 2016. Following the implementation of EMV statewide, Treasury will work with other agencies to add additional layers of protection, such as tokenization and encryption, as needed.

How the Merchant Card Plan Meets the Goals of Executive Directive 5

The Treasury's adoption of EMV technology for merchant cards meets each of Executive Directive 5's goals in the following ways:

1. **User Authentication**—EMV technology directly addresses the issue of user authentication. As agencies deploy EMV technology, the ability to ensure that transactions are occurring on behalf of the proper users will be greatly enhanced.
2. **Confidentiality**—Treasury requires our merchant card vendors to be PCI DSS (Payment Card Industry Data Security Standard) compliant. Vendors are also required to meet encryption and tokenization standards when storing card data. The current vendor—Elavon—meets all these standards and states that it meets the highest levels of PCI compliance. Data must also be kept confidential if stored at an agency. Agencies are moving forward to transfer this requirement to the vendor so that they are not retaining any card data. The terminals are directly linked to Elavon's system, and as a result, no storage is required at the agency.
3. **Reporting of fraud or unauthorized card use**—Treasury's contract with its merchant card processor requires the processor to follow Federal Regulation E for fraud cases. *Please see the Glossary for further explanation of Federal Regulation E.* The payment card processor is required to research, investigate, and report on all agency-reported incidents of suspected fraud. Consumers are directed to report suspected fraud to their credit card issuers.
4. **Data breach reporting and notification**—Section 18.2-186.6 of the Code of Virginia requires individuals or entities with certain unauthorized data breaches to notify the Office of the Virginia Attorney General and each affected Virginia resident. The merchant card processor is obligated to adhere to this law and will have to follow industry notification standards by providing notification to issuing institutions with affected card numbers.

The Commonwealth as a Disbursement Entity

In 2005, Treasury developed a prepaid debit card program to facilitate electronic payments in certain instances where the citizen had opted not to receive an automated bank account deposit. Individuals receiving these payments are no longer dependent on the delivery of checks through the mail, meaning that funding can be provided during possible emergencies, including disasters. In addition, this program provided benefit recipients without bank accounts a low cost or no cost payment alternative. Disbursements under this program currently include Temporary Assistance for Needy Families (TANF) benefits, child support payments, and unemployment benefits, as well as traditional payments such as payroll.

As of December 31, 2014, total active cards by program were:

- Unemployment Insurance 161,404
- Child Support 85,094
- TANF 65,705
- Payroll 2,537

In Treasury's lead role in facilitating card-based transactions for agencies, Treasury is working on ensuring that future prepaid debit cards issued under the Commonwealth contract are EMV cards. Treasury's current contract for the prepaid debit card vendor expires on March 31, 2016. Treasury issued a request for proposal (RFP) that requires the use of the EMV standard for the prepaid debit cards issued under the contract. Treasury has asked all offerors responding to the RFP to include an EMV implementation plan describing how the eventual vendor will ensure all prepaid debit cards will utilize EMV technology. Under the agreement, the vendor may replace all cards now, or replace cards in staggered fashion, as long as the vendor agrees to implement EMV technology in all of the cards. Treasury believes vendors will quickly roll out EMV technology in order to avoid liability shifting to the issuer. The selected vendor must have an explicit and expedited conversion process if the cards are not initially produced as EMV capable.

Treasury will allow for a staggered conversion timetable due to a potential shortage of both plastic and chips. With the shift in liability on October 1, 2015, industry suppliers of plastic and chips have been focused on meeting the demand of issuers. Credit cards have had the highest priority because fraud is much more prevalent on these cards. Most importantly, neither the Commonwealth nor the cardholder is liable for any fraud loss under our program; the service provider assumes all risk for any loss. The only drawback may be cardholders not having access to funds for a time should their card be compromised. The RFP included provisions to address and minimize this impact.

How the Prepaid Debit Card Program Meets the Goals of Executive Directive 5

The Treasury's adoption of EMV technology for the prepaid debit card program meets each of Executive Directive 5's goals in the following ways:

1. **User Authentication**—As noted, EMV technology directly addresses the issue of user authentication, which the vendor will be required to follow. Because all prepaid debit cards will soon employ chip embedded technology, the likelihood of fraudulent purchases decreases dramatically. This will help ensure that only proper users are having their transactions processed.
2. **Confidentiality**— Treasury requires our prepaid card vendors to be PCI DSS (Payment Card Industry Data Security Standard) compliant. Adhering to this standard means that vendors will be using the industry's best practices in protecting user confidentiality. These standards include protecting data in accordance with the Bank Secrecy Act and never requiring a full Social Security Numbers for routine authentication.

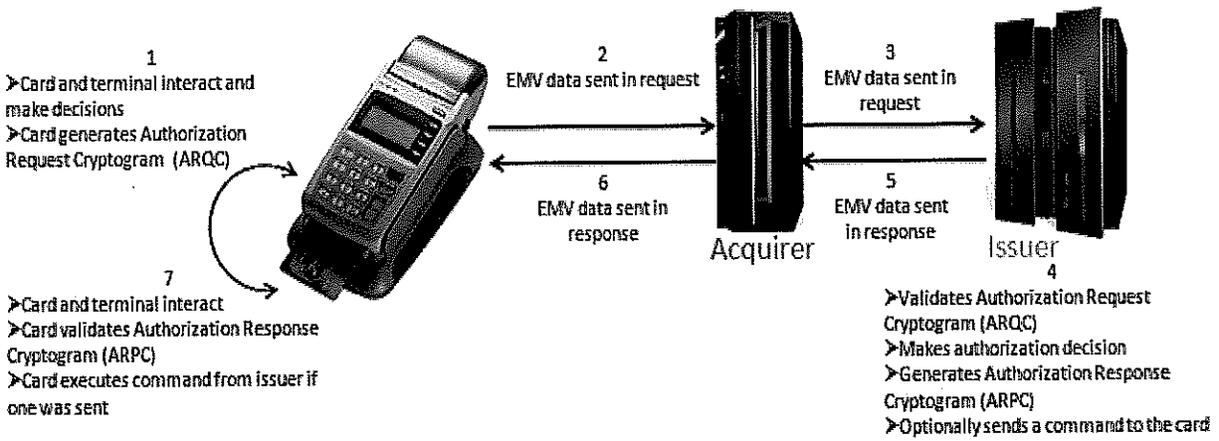
3. **Reporting of fraud or unauthorized card use**— Treasury’s contract requires the Commonwealth’s prepaid debit card vendor to follow Federal Regulation E for fraud cases. The vendor is required to research, investigate, and report on all agency-reported incidents of suspected fraud. As previously stated, the individual holder of the prepaid debit card or the Commonwealth is not liable for fraudulent charges.
4. **Data breach reporting and notification**— Section 18.2-186.6 of the Code of Virginia requires individuals or entities with certain unauthorized data breaches to notify the Office of the Virginia Attorney General and each affected Virginia resident. The vendor is obligated to adhere to this law and will have to follow industry notification standards. The vendor will have to notify cardholders and replace cards, as appropriate depending on what the data has revealed. The cardholder and the Commonwealth are not liable for any loss. The vendor assumes any loss.

Conclusion

The Treasury, in conjunction with user agencies and its card processing vendors, has already made progress in providing a more secure environment for protecting consumer financial data. Executive Directive 5 and the liability shift for payment card processors create additional incentive for agencies to move forward in a timely manner. All processing terminals should be EMV enabled by March 31, 2016 and all prepaid debit cards should be converted to chip embedded cards by December 31, 2016. By this time, all sensitive card data will no longer be held on Commonwealth systems but housed at secure vendor locations which are best equipped to protect this information. This provides the Commonwealth with the highest available industry standards for securing data and protecting consumer financial transactions.

Appendix A

Below is an illustration of the EMV authentication process discussed throughout this report. This flow chart describes the normal process that will take place whenever a transaction using a terminal equipped with EMV technology.



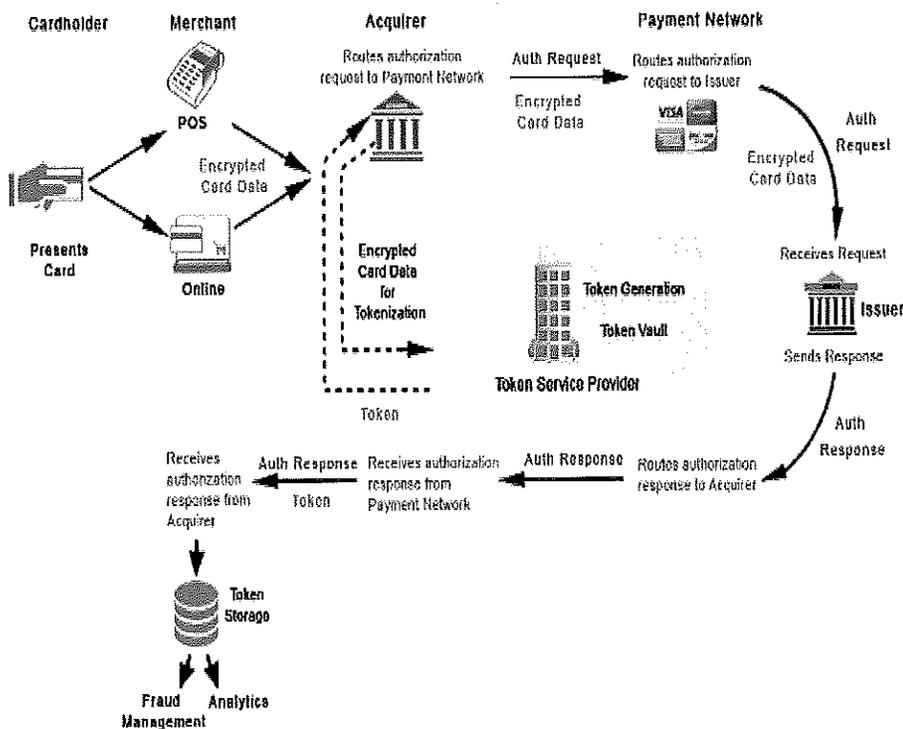
<http://www.chipcards411.com/2012/08/30/chip-card-stay-terminal/>

Appendix B

Below is an illustration of the tokenization process discussed on page five of this report. The tokenization process is only used at agency outlets that have integrated point-of-sale systems, meaning that these terminals are directly connected to that agency's financial system. Tokenization eliminates payment data from a network to ensure that a customer's sensitive payment information is safe. Tokenization replaces sensitive payment data with a unique identifier (a token) that cannot be mathematically reversed. The actual payment data is securely stored at the vendor's data centers. Typically, the token will retain the last four digits of the card as a means of accurately matching the token to the payment card owner, enabling merchants to run their systems without card data in their environment.

Token Benefits Include:

- Payment data is stored in secure data centers and exchanged for a safe token.
- Tokens are generated using proprietary algorithms and cannot be mathematically reversed.
- Token formats fit legacy payment card data fields.
- Tokens support all payment actions and checkout models, including one-time authorization, capture and settlement, recurring and subscription billing, credit and partial credit, split capture, reauthorization, and standard checkout.



<http://www.bobsquide.com/guide/news/2014/jul/22/tokenization-the-future-of-payments-security.html>

Appendix C

In addition to EMV capable technology being implemented at ABC and DMV outlets, other agencies are either in the process of adopting the most secure standard or are developing a conversion plan. Most notably:

- The Commonwealth Court system represents 270 merchant locations. Of the 270 courts, 238 locations have upgraded to EMV devices. Elavon and Treasury fully expect the remaining 32 locations to order and install their equipment by the end of October 2015, making all of the Courts EMV compliant.
- Department of Parks and Recreation is presently reviewing solutions to replace their current payment processing. The Department has a total of 40 locations and 20 are EMV enabled. Their efforts will continue during the off-season at parks while credit card activity is low. They are scheduled to have the remainder of their locations completed by early 2016.
- Department of Health's central office is overseeing the migration of all district locations to EMV technology. There are 26 locations that are EMV enabled and the remaining 89 locations have terminals ordered and in transit. The agency is scheduled to be fully compliant by October 1, 2015 or shortly thereafter.
- There are 74 (noted in Exhibit 1) other Agency merchant outlets that will require upgrading to EMV enabled terminals. Remaining agencies have been or will be notified by Elavon and Treasury by October 1, 2015 and will have a plan developed for their conversion. It is anticipated that most will be completed by the end of March, 2016. Some agencies with EMV capable terminals will need only a software upgrade to become EMV enabled. Other agencies will need to replace old terminals. There may be a delay for some agencies to convert due to budgetary constraints.

Exhibit 1
Merchant Locations

Agency Name	# of Locations to convert
Department of General Services	3
Wilson Rehab Center	1
Jamestown Yorktown Foundation	1
Corrections Adult Services	1
Sitter-Barfoot Veterans Care Center	1
Dept. of Fire Programs	1
 Colleges & Universities	
Virginia Polytechnic Institute and State University	7
Virginia State University	4
Longwood University	6
University of Mary Washington	6
Radford University	6
George Mason University	12
Virginia Commonwealth University	17
Christopher Newport University	2
Virginia Community College System	6
 Total Merchant Locations	 74

Glossary

Acquirer	Third-party service provider that acquires and processes payment transactions for merchants, manages the relationship with the global and regional payment networks on the merchant's behalf and manages the transaction database. The acquirer connects merchant transactions to payment networks and securely routing transaction from POS devices to payment network and manages from authorization to clearing to settlement.
Cardholder	End product user. One who possesses a payment card. Customer to whom the card is issued.
Card Reader	The part of a chip payment terminal where the chip card is inserted or tapped to initiate a chip transaction.
Chip Card/Smart Card	A plastic card with a chip in it that communicates information to a payment or ATM terminal.
Chip and PIN Authentication	Customer inputs a PIN to confirm a transaction.
Chip and Signature Authentication	Customer writes a signature to confirm transaction.
Cryptography	The science of protecting information by using mathematics to transform it (encrypt it) into an unreadable format. Often used to secure PINs or to authenticate an identity.
Data Breach Reporting	Applies to any entity that stores protected personal data information shall notify affected cardholders and Office of the Virginia Attorney General of any unauthorized data breaches. The entity shall also follow industry notification standards.
Digital Signature	A technique used to validate the authenticity and integrity of a message
EMV	Acronym for Europay, MasterCard and Visa. EMV is a set of standards that defines interoperability of secure transactions across the international payments landscape. The set of standards ensures payment chip cards and terminals operate successfully together.
EMV Compliant	Cards and terminals that meet security, interoperability and functionality requirements outlined by EMVCo.

Glossary Continued

EMV Liability Shift	Takes effect October 1, 2015 and any merchant or acquirers who are unable to process chip card transactions because they have not upgraded to EMV-enabled terminals could be liable for card fraud that might have been prevented with more secure technology.
EMV Terminal	Point of sale device that is able to process chip transactions.
Encryption	Encryption protects the card data by encrypting the cardholder information as it travels across various systems and networks. Encryption retains the original length and structure of card data.
E, Regulation	Provides a basic framework that establishes the rights, liabilities, and responsibilities of participants in a transaction initiated through an electronic device that instructs a financial institution to either credit or to debit a consumer's asset account.
Host	Centralized computer systems for aggregating and processing transactions. The host would typically be operated by the acquiring processor but may be operated by the merchant. Payment terminals connect to and are hosted by these systems.
Issuer	Entity or Financial Institution that issues payment data devices (Cards) to customers and performs many activities. They could be operating on behalf of client providing services.
Magnetic Strip Card	A plastic card that uses a band of magnetic material to store static data. Data is read by a magnetic strip reader. Cards that do not have a chip use the magnetic strip on the back only.
Merchant	Entity also known as Retailers that accepts payments from customers in exchange for goods and/or services and connects to a payment network through an acquirer.
Payment Network	A payment network provides POS and ATM services for credit, debit, ATM and prepaid card issuers and corresponding transaction acquirers. It establishes participation requirements, operating rules and technical specifications under a common brand(s) for the purpose of receiving, routing, securing authorization for, settling and reporting domestic and international payment transactions.
PCI DSS	The Payment Card Industry Data Security Standards.

Glossary Continued

PCI DSS Compliance	A set of requirements and best practices for enhancing payment account data security within business environments. These standards were developed by the PCI Security Standards Council, which was founded by American Express, Discover, MasterCard and Visa to facilitate industry-wide adoption of consistent data security measures on a global basis.
PIN	A personal identification number or code that authenticates his or her identity for card use.
Point of Sale	The physical location where a customer makes a payment to the merchant in exchange for goods or services.
Processor	A company that handles credit card transactions for merchant banks.
Smart Chip	A plastic card that has a computer chip implanted into it that enables the card to perform certain functions.
Tokenization	Describes the concept of using a non-decrypt able piece of data to represent sensitive data. Tokenization converts or replaces cardholder data with a unique token ID. This eliminates the possibility of having card data stolen because it no longer exists.
Triple DES	A sophisticated implementation of Data Encryption Standard (DES), in which the procedure for encryption is the same but repeated three times. First, the DES key is broken into three sub keys. Then, the data is encrypted with the first key, decrypted with the second key, and encrypted again with the third key. Triple DES offers much stronger encryption than DES.
Vendor	An entity providing a good or service.