# Fraud Reduction on EMV Payment Cards by the Implementation of Stringent Security Features

Oludele Ogundele, Pavol Zavarsky, Ron Ruhl, Dale Lindskog
Information Systems Security Department
Concordia University College of Alberta, Edmonton, Canada

***Abstract*— This paper examines the changes in the payment card environment as they relate to EMV (named after Europay, MasterCard and Visa). This research shows that if the combined dynamic data authentication (CDA) card variant of the EMV card is deployed in a full EMV environment, given the relevant known vulnerabilities and attacks against the EMV payment card technology, the consequences of unauthorized disclosure of the cardholder data is of significantly reduced value to a criminal. It also argues that it becomes unnecessary to comply with the Payment Card Industry Data Security Standard (PCI DSS) unless the merchant with the POS terminal has been exposed to proven breach and even in that case the damage caused is likely to be minimal.**

***Keywords:*** **EMV, Magnetic-stripe, Chip and PIN, PCI DSS, Payment card, Point of sale terminal.**

## 1. Introduction

At the moment, there is an estimated 1.2 billion active EMV smart cards used for credit and debit payment worldwide (of different variants, processing options and capabilities) at over 18.7 million EMV acceptance terminals [1]. EMV smart cards were designed and introduced by the banking system as a solution to the high rate of financial fraud occurring by the use of magnetic-stripe cards and also to improve the security of payment cards used in face-to-face transaction environments. A PIN (personal identification number) is used to prevent the abuse of stolen or lost cards while the chip is used to protect against card counterfeiting. The EMV chip technology is used to secure both credit and debit card transactions by authenticating the card and the individual presenting the card at the point of sale (POS) terminal and sometimes the transaction itself.

The present EMV deployment in the payment card is referred to as the "hybrid environment", in which the payment card has both a three-track magnetic stripe and the chip embedded into it. The main purpose of the chip is to securely store the cardholder data and protect the data stored against unauthorized modification and also to reduce the number of fraudulent transactions carried out with the use of counterfeit, lost and stolen cards [2], but despite these improved security measures, the payment cards are still not immune to some known attacks, many of which rely on flaws in the use of magnetic stripe information. This is due to the presence of the magnetic stripe on these cards, the values which are encrypted on the stripe and the type of the EMV variant of the smartcards used by the banking systems. At the moment, countries in Europe, North America (Canada), Latin America and Asia are all at various stages of the EMV chip migration from magnetic stripe cards except the United States, where the pressure is mounting for the adoption of the EMV smartcards for face-to-face banking transactions.

In a bid to increase control around cardholder data and reduce credit or debit card fraud via its disclosure, the Payment Card Industry Data Security Standard (PCI DSS) was introduced by the payment card networks (Visa Inc., MasterCard Worldwide, American Express, JCB International and Discover Financial Services) [2]. It was developed to protect the cardholder and sensitive authentication data wherever they are present within the environment of the payment system, providing a baseline of 12 key technical and operational requirements set by the Payment Card Industry Security Standards Council (PCI SSC). This limits the exposure of these data to criminals. This design provides an additional layer of protection for the payment card transactions. The PCI DSS is a mandatory requirement for all the entities involved in payment card processing such as the merchants, acquirers, issuers, service providers and all other entities that store, process or transmit cardholder data [3]. It aims at implementing strong security policy and infrastructure which leads to the reduction of the risks of security breaches [2]. The PCI DSS standard is however only effective if the payment system environment in which the payment transaction is being performed is in full and continuous compliance with the PCI DSS requirements, else security breaches are inevitable.

In this paper, we will show by the comparative analysis of the security features of the different variants of the EMV payment cards, in order to describe how the CDA variant of the EMV chip technology can overcome known successful attacks and vulnerabilities against the EMV technology. Lastly, we will argue that it is not necessary to comply with the Payment Card Industry Data Security Standard (PCI DSS) when the CDA card variant of the EMV is deployed in a full EMV environment for POS transactions.

The structure of this paper is as follows: In Section 2, we provide an overview of the EMV card personalization and the EMV transaction process and the different variants of the EMV payment cards. Various forms of attack against the different variants of EMV payment cards and the consequences of unauthorized disclosure of cardholder data in hybrid and full EMV environments will be described in Section 3 and Section 4 concludes with the impact of the implementation of the CDA cards in a full EMV environment on the PCI DSS as regards to the compliance of organizations to the standard.

## 2. An Overview of the EMV Card Personalization, Transaction Process and the Different Variants of EMV Payment Cards

In this section we will give an overview of the EMV card personalization and the EMV transaction process. We will also compare the security features of the different variants of the EMV payment cards.

### 2.1. EMV Card personalization

All the payment card issuers generate EMV cards by verifying customer information and then create a personalized Chip and PIN capable card. On the front of the card are personal details such as name, the Primary Account Number (PAN), expiry date and occasionally other numbers. Then the data for the Chip and magnetic stripe is created. This is first created by having the personalizing machine choose a PIN at random. Then, using a one way cryptographic function, a variety of known values about the bank, the PAN and the customer. The PIN created is then used to create a PIN Verification Value (PVV) which is how the PIN is stored on the magnetic stripe (i.e. not as a PIN directly but as a one way value which can only be compared to a similar calculation by input at a POS terminal and then comparison with the value on the chip or the value the bank has stored). This same process is performed with a different combination producing a PIN Verification Value for the ICC (iPVV) and this is placed on the chip. Both values are also stored by the issuer on their back end secure computer after the personalization is finalized [4].

This personalization results in storing the PIN in such a way that a comparison can only be done when the same one way process which produced the PVV is run again (by the POS and using the missing element, the PVV, which only the cardholder knows and can provide during the POS process.)

At the end of the personalization process the personalization machine tests the card and once these tests are complete, the personalization process prints a letter to the customer and includes the PIN in the letter. The PIN is normally covered in some secure way and must be taken apart or peeled off by the customer after receiving the card. Tampering would be self-evident to the customer receiving the card [4].

In this final step, the printing of the PIN is the only place where the PIN is ever printed and the printing must be done inside the personalization machine and not visible to humans. These steps are intended to produce the result that the PIN is not seen or stored by anyone or any computer except the customer and that the card and the bank rely on reproduction of the IPVV or PVV by way of running the one way function again using the input from the POS terminal where the customer uses their PIN (initially contained in the letter).

Because of the importance of the values, most issuers require customer PIN changes to be done only at branch locations of the issuer where a more secure terminal can be used to modify the PIN and store it as new PVV and iPVV values in the backend computer of the bank. This is often done in combination with an issuing bank ensuring the PIN change is done correctly while it stores new PVV and iPVV values.

### 2.2. The EMV Transaction process

During an EMV payment card transaction, the chip on the smart card must make contact with the chip reader in an acceptance terminal (e.g. POS terminal). This terminal connection could be either contact or contactless. For the contact method, there must be a physical contact between the chip and the card reader for transaction to occur while for the contactless, the chip is required to be within sufficient proximity to the card reader for information exchange between the chip and the acceptance terminal [2]. The EMV specification details the technical requirements for chip embedded payment cards and for the various point-of-sale infrastructures. In the EMV chip technology, if the transaction is approved, the Integrated Circuit Card (ICC) generates a Transaction Certificate (TC) which is passed to the terminal and used to claim payment during the clearing process.

On the other hand if the transaction is declined, the ICC generates an Application Authentication Cryptogram (AAC) message. If the transaction needs to be approved online, the ICC generates either an AAC or Authorization Request Cryptogram (ARQC), which is sent to the issuer (e.g. the cardholder's bank). The issuer replies with the Authorization Response Cryptogram (ARPC) message signifying whether the transaction should be approved (the ICC generates the TC message) or declined (then the ICC generates the ACC) [5]. The terminal manages the level of risk by requiring certain transactions to be authorized online instead of being authorized locally in order to safeguard against fraudulent use. This includes checking the transaction amount against the floor limits, detecting when the defined limit of consecutive offline transactions have been reached and in addition, offline-capable terminal will also randomly select certain transactions to be performed online. The online processing (depending on the variant of the EMV chip card used) allows the card issuer to analyze the transaction details and to decide whether to go ahead with the transaction or reject it. This provides the issuer with the opportunity to check the account status and apply criteria based on the acceptable limits of risk predefined by the issuer, the acquirer and the payment scheme (e.g. Visa, MasterCard). If a valid response is received from the issuer, the card analyzes the result of the online processing, authenticates the data received from the card issuer and request the terminal to complete the transaction by either declining or accepting the transaction based on the result of the online processing. Therefore, the card cannot request the acceptance of the transaction if the issuer declined the payment [2]. At the completion of the transaction, the card is removed from the chip-reading device.

In summary the payment transaction process of the EMV protocol can be divided into three phases namely card authentication, cardholder verification and the transaction authorization. The card authentication phase assures the terminal of the legitimacy and authenticity of the card. This is done by terminal access of the CA signed certificate containing the cardholder data contained on the printed face of the card. This certificate must be on the embedded chip to be validated as a genuine card. The cardholder verification phase confirms to the terminal that the cardholder knows something that only they should know about the card.

A PIN entered by the cardholder is put through a one way function producing a value which matches the one assigned to the card through the personalization process the issuing bank uses when the bank creates the card. The PIN (value) is stored on the secure area of the chip and it may be changed at both the bank and the secure area of the embedded chip. Changes to the PIN values stored on the chip and the bank must be completed by the cardholder in a secure terminal and this is normally a bank's own terminal. The transaction authorization phase reassures the terminal that the card issuer (i.e. the bank)

approves the transaction by placing a certificate with transaction details in the approval message and in some cases by placing message authentication code over the entire transaction details during the transaction approval process.

## 2.3 The Different Variants of the EMV Payment Cards

The payment card issuer (i.e. the cardholder's bank) selects the EMV card variant to use and also have the autonomy to choose the subset of the EMV protocols that will be implemented on the card. The specific implementation of the EMV standard that a bank has used is normally placed on the issuing banks' website as others involved in processing must know the specific cryptographic choices used by the bank. This includes making decisions concerning the digital signature methods, message authentication code (MAC) algorithm to be used for the card processing, card authentication and risk management options; ensuring that the selected options comply with both the payment card network rules the EMV framework, and the related terminal hardware and software [6]. The EMV specification defines three main types of card authentication methods otherwise known as variants of the EMV chip card namely, the static data authentication (SDA) card, dynamic data authentication (DDA) card and the combined dynamic data authentication (CDA) card [7]. The EMV chip technology supports cardholder authentication through the use of Cardholder Verification Method (CVM) and ICC authentication by the use of the SDA, DDA or CDA cards [5]. Although the EMV specification supports signature authorization, the PIN verification method remains the dormant method used for the CVM.

Table 1 shows the different variants of EMV smart cards emphasizing the basic characteristics that differentiate each card from the other. The SDA card is a cheaper alternative for the banking industry considering the cost of production because SDA uses only a symmetric key on the card (stored in the secure area of the chip), which is shared only with the issuing bank. The drawback with the use of the SDA card is that it is susceptible to the various successful attacks as evident in [2], [6], [8], [9]. The terminal sends a summary of the transaction data once the PIN entered by the cardholder is verified by the card and the MAC is generated using the shared symmetric key with the issuer. The SDA card can only prove a payment card is genuine only if the terminal is online (i.e. connected to a bank via a network). The SDA submits a static cryptographic certificate to the terminal, incorporating the primary account number (PAN) and a digital signature when performing card authentication [10]. The SDA cards are found to be even less secure when used with an offline terminal as compared to when the magnetic stripe cards are used, since it is the duty of the payment card to verify the PIN and reply with a "yes" or "no" to the POS terminal. The SDA cards can be easily cloned and can be used by criminals to perform fraudulent offline transactions because of the lack of mutual authentication with the above described authentication of the card.

The issuer has a public-private key pair used for asymmetric cryptography if the transaction is required to be performed offline by the payment card. The POS terminal only knows the public key of the issuer because of the high risk involved in putting both keys on the terminal which could result into fraud if discovered. The certificate which contains the public key of the issuing bank is the only requirement the terminal needs to evaluate if the card is genuine.

**Table 1. The Characteristics of the Different Variants of EMV Smartcards**

| Static Data Authentication (SDA) Card | Dynamic Data Authentication (DDA) Card | Combined Dynamic Data Authentication (CDA) Card |
|---|---|---|
| Can prove a card is genuine online only. | Can prove a card is genuine either online or offline. | Can prove a card is genuine either online or offline. |
| Has only certificate of static data signed by issuer and certificate of issuer signed by CA | Has same certificate of static data as SDA, Has a "card level" public key signed by issuer, and certificate of issuer signed by CA. | Has same certificate of static data as SDA, Has a "card level" public key signed by issuer, and certificate of issuer signed by CA. |
| Signature remains the same every time the card is authenticated. | Signature is only valid for authentication instance | Signature is only valid for authentication instance |
| Digital certificate is signed by issuer's private keys. | Digital certificate has public key of card and the private of the "client level" card stored in a secured area of chip | Digital certificate has public key of card and the private key of the "client level" card stored in a secured area of chip |
| Support only symmetric cryptography, Terminal must have CA Certificate. | Supports asymmetric cryptography as well. Terminal must have CA Certificate. | Supports asymmetric cryptography as well. Terminal must have CA certificate |
| Card cannot protect itself against cloning and certificates for messages. | Able to generate digital certificate combining the time of transaction and card, cardholder and merchant details for each transaction. | More advance than the DDA card, able to generate digital certificate combining the time of transaction and card, cardholder and merchant details for each transaction. It also combines a dynamic signature and an application cryptogram and the data (MAC) signed by the card include a random number provided by the terminal and the ARQC. |

For the DDA cards more complex cryptography is used in that the chip in the card can also do asymmetric cryptography and have a public-private key pair assigned to the card itself. The private key is held only in the secure area of the chip and cannot be accessed by the terminal. The public key of the card is verified through a signed certificate of the public key of the card signed by the issuing bank. DDA involves a challenge-response mechanism to prove the authenticity of the card by using a private asymmetric key ($S_{IC}$) to sign a challenge chosen by the terminal and sent to the chip. If the terminal can verify that both the card and the information on the card (by access of bank certificate and the card certificate) have not been altered and also prove that the card is not a copy of the original card issued (cloned cards being one of the attach vectors in compromised SDA cards above). One of the additional strengths of the DDA card is that the above can be verified whether or not the card is online since the chip can sign a challenge correctly and by doing so validate both using the

bank and the cardholder details. Signing of the challenge from the terminal successfully (card verification) allow the terminal to proceed to the next phase of PIN verification.

Although the DDA card mechanism is used to prevent card cloning and to authenticate the genuineness of the card it does not protect the subsequent transactions performed by the card [12]. The DDA and the CDA cards are capable of performing dynamic data authentication (by using the private key in the chip to correctly sign challenge data) while the SDA card can only perform static data authentication as it is not capable of asymmetric cryptography. The unique feature of dynamic data authentication is that it prevents the transaction data from being fraudulently reused even if it was stolen from the processor's or merchant's database thereby making the data of little or no use to the criminal.

The CDA cards have this advantage over the DDA cards, in that the message signed by the ICC which includes an additional Application Cryptogram (AC), which is used to protect and validate the specific transaction messages (amount, time, etc) generated during the transaction. The ICC uses the AC Session Keys (derived from the ICC AC Master Key, shared only between the ICC and the card issuer) to place this MAC on the transaction details. The ICC AC Master Key is unique per card and it is derived by a combination of the cardholder's PAN, the PAN sequence number and the issuer Master Key. The sequence number of the PAN is used to identify a specific card among several cards owned by the same bank customer with the same PAN [5]. This advance feature of the CDA card gives it the ability to overcome sophisticated types of attack at the POS terminal which is very difficult for both the SDA and DDA cards to surmount and thereby making the CDA card the most secure and the best alternative for use in EMV chip cards. With CDA we have strong card verification by use of two certificates (one for the bank and one for the card itself), strong challenge and response (either online or offline PIN verification), and strong transaction verification using MAC code secured by the symmetric key shared only by the bank and the ICC chip (in the secure area of the chip).

## 3. A Survey on Attacks against Payment Card and Consequences of Unauthorized Disclosure of Cardholder Data

In the magnetic-stripe environment, data which are embossed on the surface of the payment cards are also be stored in the magnetic strip. These include the cardholder's name, expiry date, card number and other necessary data such as the card verification value (CVV) of the card [10]. The magnetic stripe becomes easy to clone, once the data content of the magnetic stripe has been copied by a fraudster. Moreover, the function of the swipe (at a terminal with allows swiping the magnetic strip) is to copy all the data from the strip. Obviously, as discussed previously, this means that all terminals which allow swipe operations gain access to all cardholder details. The detail include the PAN information from the customer (everything on the front of the card) and the one way function used to store an PVV after application of PIN knowledge in an interface (terminal). This section will examine various attacks carried out in the hybrid environment and the possibilities of the success of the same kind of attacks in a full EMV environment in relation to the consequences of unauthorized disclosure of cardholder data.

### 3.1. Various Attacks against Payment Card in a Hybrid Environment

The various attacks against the payment card in the hybrid environment can be viewed as either cross-border or domestic frauds. The cross-border frauds are fraudulent transactions that are performed by criminals with the use of the payment card outside the country in which it was issued to the cardholder while domestic frauds are fraudulent transactions performed by criminals with the use of the payment card within the country in which it was issued.

The attacks applicable in cross-border frauds include attacks that rely on the fall back mechanisms of the magnetic stripe, which have been proven successful due to uneven migration to the EMV payment cards in various regions of the world. Fraudsters intensify efforts on compromising the magnetic stripe data so as to fraudulently use the POS terminal in regions yet to migrate to the use of the EMV payment cards.

In the hybrid environment, cross-border fraud can be performed when the chip on the payment card presented at the POS terminal has been damaged or is unreadable. The terminal falls back to the magnetic stripe operation of the payment card, and this makes it possible for a fraudulent merchant to skim the customer's payment card successfully, using the obtained cardholder data to make a counterfeit card provided that the PIN has also been recorded as well. This means that a fraudster who is not able to clone the chip will simply copy the magnetic stripe to make a counterfeit card, which operates just like a legitimate card from the perspective of the terminal and transaction is permitted to proceed [9], [10]. The use of cloned payment card on the POS terminal has a high rate of success when the terminal is offline and the EMV chip variant is a SDA card. The fraudster does not even have to know the PIN, once a counterfeit card is made; he simply programs the payment card to say "yes" in response to PIN verification request irrespective of the PIN entered at the terminal [9], [10]. This type of attack is called the replay attack (also referred to as "yes cards"). It is important to note here, that if the cloned card is an SDA chip card from a magnetic stripe, the replay attack will not work online, since the PIN used will certainly not be correct (unless social engineering was used) otherwise the PVV will not be correct after comparison with the online issuer in the card authentication phase.

A similar attack method can also be done by using a stolen card that has both the chip (SDA) and magnetic stripe embedded in it in an environment where the POS terminal permits only the use of the magnetic stripe, which then enable the card to bypass the chip mechanism and fall back to the magnetic stripe operation. What enhances this attack is that the fallback mechanism in this situation tend to be less robust than the magnetic stripe mechanisms are in the environment where the magnetic stripe is the main technology used [9].

The attacks used for domestic frauds in the hybrid environment include damaged/unreadable card chips, replay attack, eavesdropping of the POS terminal, POS terminals with poor anti-tempering mechanisms, the man-in-the-middle attack, untrusted user interface, the back end API (Application Program Interface) attacks at the bank data center and finally the attack implemented during card-not-present transaction, which can also be used for cross-border fraud.

Attacks used for domestic frauds in the hybrid environment include the eavesdropping of the POS terminal. Once the account and PIN data can be eavesdropped from a transaction made by an EMV card at a POS terminal, it becomes easy to make a magnetic stripe containing that data for a fraudulent use in an environment where EMV chip technology is not

supported. Alternatively, the fraudster can intercept the communication between the POS terminal and the chip to copy the magnetic stripe, and can also obtain the PIN entered by the customer as it is sent to the chip during the cardholder verification stage (i.e. if the PIN is sent to the chip in plaintext) [10]. There are various approaches by which the eavesdropping can be done but one of the preferred approach in terms of cost, development time and convenience is to create a skimming device (i.e. POS terminal skimmer) that conveniently sits on the smartcard slot of the POS terminal and used to capture the card and PIN data without the suspicion of the cardholder. In conducting this attack the attacker may purchase something with their card and while the POS clerk is distracted, the skimmer is inserted. This type of attack is usually employed to capture and store account details of majorly SDA cards in large quantities and this device can be removed quickly from the terminal should there be a problem or suspicion [13].

The POS terminals cannot be fully relied upon because they are viewed as being under the control of the potentially untrusted merchants and their proper functioning cannot be fully guaranteed and for this reason they are tamper resistant to prevent malicious merchants or staff from extracting cardholder data. Nevertheless these terminals are still prone to attack due to poor anti-tampering mechanism and research has shown that it may not even be necessary to open the device to do so; manipulating the power supply or transmitting a radio signal may be sufficient [13]. Most of these attacks are possible due to design errors in the tamper resistance protection measures discovered in some of the POS terminals and thereby making it possible to circumvent the protection in place [2]. Drimer et al in [10] demonstrated that some of the POS terminals have inadequate tamper resistance, and therefore a possibility of adding a tapping device to record the cardholder's PIN and necessary details to allow a cloned magnetic stripe card to be produced [6]. The man-in-the-middle attack which was discovered to be successful in the hybrid environment, allowed the use of any payment card (e.g. stolen/lost) without the knowledge of the card's actual PIN as demonstrated by Murdoch et al in [6]. The "man-in-the-middle attack" (a.k.a. the wedge attack) is found to be effective against both offline and online transactions. This type of attack is possible because of the central flaw discovered in the EMV protocol used in the payment cards in the UK, in which the PIN verification step is never explicitly authenticated [6]. Since the POS terminal is permitted to communicate directly with the legitimate card during card authentication, with the use of a stolen card, a man-in-the-middle attack can be used to intercept and modify the communication between the stolen card and the terminal so that during the cardholder verification, the man-in-the-middle suppresses the messages as they are being sent to the stolen card. Therefore, irrespective of the PIN entered by the fraudster the man-in-the-middle tells the terminal the PIN entered is correct and the transaction is authorized to proceed. This attack is also successful when the transaction is done online, which is due to the oversight of the design of the transaction authorization stage. It was discovered in the EMV specification that the ARQC (Authorization Request Cryptogram) and TC (Transaction Certificate) messages include the result of the cardholder verification but the result only indicate whether the verification was attempted but failed, but does not distinguish if the verification succeeded or if it was not attempted at all. Therefore, there is the high possibility that the man-in-the-middle can suppress the cardholder verification and then relay the ARQC and TC between the legitimate card and terminal. So when the issuer receives these cryptograms, the authorization would succeed because the cryptograms are seen as being sent from a legitimate card and the bank would accept the transaction [10], [20].

Another concern when considering the hybrid environment is the user interface trust issue. This in fact, questions the assurance of the cardholder concerning the amount displayed on the POS terminal during a transaction. What if the POS terminal has been compromised? When the cardholder puts the card in a POS terminal, what is the guarantee that the payment card is genuinely interacting with the terminal? This serves as an advantage for a fraudster to implement a relay attack. This is a situation whereby the POS terminal has been compromised by a fraudulent merchant and the unsuspecting cardholder is made to authorize payment for another transaction done elsewhere, while thinking that the payment being made is based on the current transaction done at his present location [2], [9]. The relay attack is done successfully because the compromised terminal appears legitimate to the untrained cardholder, who gets fooled easily without suspicion. The relay attack is outlined in [9] and demonstrated by Drimer and Murdock in [2].

Also, the dotcom boom which has resulted into huge activities of card-not-present transactions during online shopping, attacks which make use of "phishing attack", aimed at capturing online banking details of customers, perpetuated by sending emails impersonating banks, asking customers to click a link under false pretense that their accounts have been compromised, and when they do, a malicious copy of their bank's website asking for their account details or authentication data is displayed. This form of attack on the EMV chip cards result into online fraud and have been reduced with the use of Chip Authentication Program (CAP) introduced by the banks [14], [2]. EMV was adapted to the CAP protocol and used to generate codes for two-factor authentication [2]. Another common attack for online transaction involves the use of malwares in which authentication details are stolen by a software key-logger installed on the customer's computer [14]. Other social engineering tricks – by telephone or post (this is by brazenly calling up customers and asking for their PIN or CVV or using postal redirection scams) [2], [9].

The '3-D Secure' protocol was also introduced by Visa (Verified by Visa) and MasterCard (MasterCard SecureCode) to help reduce online fraud during card-not-present transactions. It is essentially a single-sign on system. Although it has flaws in its implementation, it was adopted easily by merchants because of the contractual terms of liability which offered reduction of liability in case of disputed transaction for merchants [2].

#### 3.1.1. Consequences of Unauthorized Disclosure of Cardholder Data in a Hybrid Environment

The consequences of unauthorized disclosure of the cardholder data in a hybrid environment, differs based on the variant of the EMV payment card used. It should however be noted that in the hybrid environment, the common payment card in use are the SDA and the DDA cards [1], [6], [15].

When the SDA card is used, the consequences may be the successful cloning of payment cards by taking advantage of the fallback mechanism to copy the magnetic stripe, the use of skimming devices to eavesdrop on the POS terminal to capture

and store account details and PIN of the card made possible by the presence of the poor anti-tampering mechanisms [2], [13]. In reality, the consequences of unauthorized disclosure of cardholder data relate to the risk involved if the PIN and card details are intercepted when they are sent unencrypted between the card and the PIN entry device (PED) during a transaction, a fake magnetic stripe card can be produced by fraudsters and due to the backward compatibility of the EMV smartcards, the possibility of falling back to the older system if the chip is damaged or unreadable [11], [13]. Since the PEDs are expected to protect both the cardholder's PIN and card details, the presence of vulnerabilities in the PEDs will lead to disclosure of cardholder data which indicates a high risk of fraud of which the cardholder will still be held accountable in most cases because he would have entered his PIN during the transaction. It was also discovered that the PEDs appear to protect both the merchants and banks secrets while leaving the cardholder's card details and PIN inadequately protected [11], [13].

When the replay attack is used in the case of a SDA card, the attack is easily successful with the unsuspecting cardholder entering the PIN willingly to authorize the transaction while if the DDA is used, the relay attack will not be successful because of the challenge-response mechanism built into the chip [12]. The consequences of unauthorized disclosure of cardholder data with use of the replay attack on SDA cards will result to successful fraudulent transaction done by criminals with the use of cloned SDA cards.

However, the man-in-the-middle-attack as demonstrated in [6] will still be successful against both the SDA and the DDA cards because the terminal cannot verify the transactions performed by these types of EMV chip variants when an offline PIN verification method is used. The success of this attack could be attributed to the cardholder verification phase, in which the offline PIN verification is not authenticated. This hereby enable a criminal to use man-in-the-middle attack to trick the terminal in such a way that any PIN entered is accepted as correct while the card concludes that the CVM was done by the cardholder signature option. The consequences of unauthorized disclosure of cardholder data with use of the man-in-the-middle attack will result to the ability of criminals to modify the transaction elements to perform successful fraudulent transactions without entering the valid PIN number. Also, in the case of resolving disputes between the cardholder and the bank over a transaction, the reliability of the EMV smartcard technology and the evidence generated has become increasingly important. In a situation whereby, the man-in- the-middle attack is used by a criminal to compromise a genuine payment card of a customer. When the defrauded customer eventually notifies the bank of the unauthorized transaction, the disputed transaction is often reversed under the old system (i.e. the magnetic stripe) but in the EMV chip technology, the bank may alternatively believe that the customer has acted negligently by not protecting the payment card or PIN adequately or both the card and PIN. If such a decision is challenged, the bank frequently sees the EMV chip technology as infallible, stating categorically that the customer's payment card was read and the PIN was used for the transaction thereby concluding that the customer must be grossly negligent or lying. In other words, in resolving disputes, the consequences of unauthorized disclosure of cardholder data makes it difficult for the customer to obtain refunds once the transaction made was authorized by PIN except when proved otherwise by fraud experts. Anderson et al [9] described how cardholders might have difficulty in obtaining refunds when a fraudulent transaction was proven to have been authorized by PIN. Furthermore, in the case of a disputed transaction, if the transaction was authorized by a signature the merchant will be held liable for fraud while if the same transaction had been authorized by PIN, the cardholder is liable for fraud [6]. Arguably, the bank is expected to show that their position is defensible and that the transaction was not performed by a third-party fraudster exploiting a security vulnerability of the system [6], [10]. Murdoch et al [6] described and demonstrated the EMV flaw that allowed fraudsters to use a genuine card to make fraudulent transaction without knowing the card's PIN and to be undetected despite the fact that the merchant has an online connection to the banking network and thereby making it evident that the fact the terminals print "verified by PIN" does not mean that the valid PIN was entered for that particular transaction [6].

In an attack done with the use of replay, the customer is not expected to lose money but if it was done offline the merchant will be held accountable for this kind of fraud because he will be accused of negligence once the fraudulent transaction is reversed, for not verifying transaction with the issuer of the card before proceeding with the transaction [10].

Ultimately, the issue of liability shift (from the payment card issuer to the cardholder and merchant) was never considered as significant under the magnetic stripe technology because the cardholder can always complain when he suspects a fraudulent activity on his bank statement or when charged wrongly for a purchase, but under the hybrid environment, the conditions are totally different, and the liability has shifted from the payment card issuer (bank) to the cardholder and the merchant [6], [11] therefore making the consequences of unauthorized disclosure of cardholder data very serious as relate to the cardholder and merchant when exploited by criminals.

### 3.2. Possible Attacks against Payment Card in a Full EMV Environment

In a full EMV environment, the magnetic stripe will be removed or phased out from the payment cards, and only the chip will be used for business transactions at the POS terminal. Technically, in a full EMV environment, frauds that are perpetuated by taking advantage of the presence of the magnetic stripe in the hybrid environment such as the use of fallback mechanism and card cloning will be drastically reduced [20]. In essence, EMV implementation that utilize the different card verification values present on the chip Card Verification Value for ICC (iCVV) from those available in magnetic stripe image Card Verification Value (CVV) will prevent the cloning of payment cards from compromised EMV magnetic stripe-image data and also limit the impact of lost/stolen/mail not received types of fraud [11], [20].

EMV does not protect the confidentiality of or the inappropriate access to sensitive authentication data and/or cardholder data during any point of the transaction at the POS terminal [20]. This is because the PAN is needed to be processed in clear text to complete critical steps in the EMV transaction. The data elements of the cardholder include the PAN, cardholder name (which is not required to be transmitted) and expiration date. These are all visible on the surface of the payment card, except the service code which is only present in the Track 2 Equivalent Data on the chip. The PAN is sent in the clear during EMV transaction in order to identify the

cardholder and facilitate the transaction routing, enable key derivation and perform data authentication at the POS terminal. The expiration date is sent in clear text during an online authorization and is included in the Track 2 Equivalent data. The data elements of the sensitive authentication data for a full EMV transaction are the ICVV and the PIN [20]. The EMV specification allows for offline verification of the cardholder through the use of the PIN, the online PIN verification for the cardholder verification is also supported depending on what is required in the CVM process and also the presence of the iCVV stored on the EMV chip card will prevent the production of counterfeit cards [20]. This means that in a fully EMV environment, the SDA cards will no longer be vulnerable to the well-known replay attack because the PIN, along with the other card information cannot be used to create a counterfeit magnetic stripe version of the card [2], [6], [20] but still the SDA card is not a good option to be used in a full EMV environment because it can only use the PIN to verify the cardholder only when it is online (i.e. connected to the bank network in real-time) and it will still be vulnerable to attacks, such as the man-in-the-middle attack and cannot also resolve the user interface trust issue experienced because this type of card is only verified by the static digital certificate signed by the issuer that it presents to the terminal. It cannot also do RSA asymmetric cryptography and thus cannot sign any transaction with a private key.

For the EMV chip technology, one of the PIN algorithms used is the VISA PVV. It is the cryptographic signature of the PIN and other cardholder data. Using VISA PVV algorithm with 3-DES encryption is considered very resistance (very difficult to brute force) and is regarded as secure, therefore making the chip impossible to counterfeit. The encryption process it involves serves as an antifraud mechanism. L. Padilla made a demonstration of the attempt to brute force VISA PVV algorithm with DES encryption in [2]. The DDA cards can do RSA asymmetric cryptography and also involves a challenge-response mechanism to prove the authenticity of the card by using a private asymmetric key, $S_{IC}$ to sign a challenge chosen by the terminal. It can prevent the replay attack in an offline transaction but not the man-in-the-middle attack and cannot resolve the user interface trust issue. This is because the DDA card cannot prove the authenticity of a transaction done by a card, in such a way that it is able to verify that the transaction was done by that particular card since it was not designed to have that ability.

In the EMV transaction process, after inserting the ICC of the card into a terminal [6], it boots the chip and starts to process data after issuing a reset to the ICC chip. The ICC chip then begins to read chip information (various signed and unsigned data contained in the SDA, DDA or CDA chip). The PAN data is included in this. While some records must be signed or provided by certificate, others are optional. In SDA, signed data is contained in the certificate on the card for the cardholder (which can be verified by the terminal through the CA certificate which must be at the terminal. DDA and CDA have RSA keys for both the issuer and the card itself and the card RSA card public keys are chained up to the issuer with a certificate. As with SDA the terminal can verify the chained certificates by reference to the CA certificate at the terminal. Once the card has been verified the get processing options command is completed and records returned with a list of things the card can do and the card verification method list (the way the client will be verified). This list can be signed by the issuer (in SDA) or the card itself (DDA or CDA) and if signed the list can be verified by the terminal through reference to the certificate chain and the CA certificate at the terminal [7], [12]. Regardless of the list being signed or not, the terminal still uses the list to provide a menu or to provide only one option (for example if the terminal can only perform a purchase transaction).

Manipulation of the get processing options list and card verification method may occur in cases where this data is unsigned. The additional cost to sign this data during the personalization phase would greatly assist all three card types in protecting the terminal manipulation of secure processing options [7], [12].

The man-in-the-middle attack can be eliminated in the full EMV environment with the use of the device called "Smart Card Detective" as demonstrated by Choudary [8]. This same device can also help to resolve the user interface trust issue due to the flaws discovered in the PED used for payment by the customer to the merchant [2]. This device is able to intercept the communication between the card and the terminal and therefore can provide the cardholder with the ability to observe the amount requested by the terminal and the option to continue or reject the transaction based on the cardholder's discretion. This experiment is demonstrated in [8], and further used for test scenarios in [2]. For Choudary's experiment, a specially designed chip card was used but without the magnetic-stripe, and it was built on the same ISO 7816 standard as required for any EMV chip card, so as to make it compatible and also provide necessary functionality.

Alternatively, the man-in-the-middle attack will not be successful against the CDA card because during the cardholder verification stage, the CDA combines the authentication of the card with actual transaction done with the card which will result in the issuer authorizing the transaction therefore any alteration of the transaction elements implemented by man-in-the-middle attack will invalidate the signature on the message generated by the card and the transaction will be denied [12].

Therefore, the CDA card can also be used to eliminate the man-in-the-middle attack, relay attack and also resolve the user interface trust issue in a full EMV environment. This is so, because once there is any alteration in the elements of the transaction, the issuer will not authorize the transaction because a different message will be generated by the card which will not correspond with the message received by the issuer [12].

The relay attack demonstrated by Drimer and Murdock in [2] will be successful against SDA or DDA chip card but not against the CDA chip card because the CDA chip card computes a MAC, encrypting it with $K_{MAC}$ (i.e. the key of the MAC) over the details of the transaction and interestingly $K_{MAC}$ can only be computed by the chip in the card and the issuer. Therefore, any cardholder data or sensitive authentication data extracted by a fraudster during an EMV transaction such as PAN will be of reduced significant value, due to the dynamic nature of the CDA card because the value (amount) of the transaction coupled with the PAN and the transaction and all these are encrypted with the MAC so the cardholder cannot buy beyond the amount specified in the transaction number and thereby preventing the success of the relay attack. This explanation is also applicable to the man-in-the-middle attack and the user interface trust issue. With all these major successful attacks experienced in the hybrid environment being solved with the use of the CDA card variant of the EMV cards, the CDA card is the most preferred EMV smartcard [12], that all banks will eventually want to migrate

to, coupled with reasons such as the card can verify the legitimacy of the card being used by the cardholder; the assurance that the cardholder knows the PIN and that the transactions have message authentication code (MAC) so that they can't be relayed and misrepresented because the only place the secret key is on the secured area of the chip and with the card issuer (i.e. the bank). Only the bank can recreate the key at any time because it has the master key and it created the symmetric key by the formula it applies to the customer details and their master key. The EMV protocol itself is indeed robust and can be adapted to different technology in the face of changing business demand as explained in [2].

#### 3.2.1. Consequences of Unauthorized Disclosure of Cardholder Data in a Full EMV Environment

The consequences of unauthorized disclosure of the cardholder data in a full EMV environment is reduced to a significant extend because it is difficult to make a copy of the original chip on the card [2] and also in a full EMV environment, a chip-generated dynamic data element is done uniquely by the use of the CDA card for each transaction made in a face-to-face transaction, coupled with a robust authentication process for card-not-present (CNP) transaction, this makes it difficult to create counterfeit cards even if the cardholder data (e.g. PAN) or authentication data (e.g. PIN) is sent in clear-text. EMV transaction is therefore capable of reducing fraud value of cardholder data and preventing the compromise of sensitive authentication data [12], [20]. This situation helps to prevent the fraud liability from being dumped on the cardholders or merchants by the banking industry as opposed to the practice in the hybrid environment.

Even in a situation in which the cardholder data is compromised the consequences of the unauthorized disclosure of the data in a full EMV environment with the deployment of CDA card is significantly reduced in that the breach of the cardholder data confidentiality cannot be used for fraudulent transaction by criminals.

The implementation of the CDA variant of the payment card also help to provide valid evidence of transaction in case of a transaction dispute between the cardholder and the merchant which may also involve the issuer or acquirer. It also helps to protect the payment card system from abuse by any of the parties involved in any transaction.

Given the above findings about the consequences of unauthorized disclosure of cardholder data in a full EMV environment compared with that of a hybrid environment, we can come to the conclusion that the consequences of unauthorized disclosure of cardholder data in a full EMV environment in a face-to-face transaction is significantly reduced because of the ability to protect MAC message with a symmetric key and protect authentication with an asymmetric key.

But it should be noted that as the technology improve so also will criminals move with the trend with time. However, this research is not intended to focus or put into consideration the privacy legislation in certain regions of the world, in which the privacy law may prohibit the disclosure of the full PAN of the cardholder, in a bid to protect the private/personal information of the individual presenting the card. In such an environment, this research will likely be viewed from the perspective of privacy rather than for security reasons.

## 4. The Impact of a Full EMV Implementation on the payment card Industry data security standard (pci dss) Version 2.0

In the guidance document, "PCI DSS Applicability in an EMV Environment", published October 5, 2010 by the PCI SSC. It was stated that should EMV (i.e. EMV-only card) become the sole means of payment in face-to-face transaction coupled with a globally adopted robust authentication process for CNP transactions, the need to keep the PAN and other sensitive data confidential would be significantly reduced [20].

Having recommended the use of the CDA variant of the EMV card for a full EMV environment and established its relevance, we will show how the implementation of a full EMV environment will impact the PCI DSS v 2.0. However, the need to understand the POS transaction authorization in the different payment card environment is necessary in order to know the various stages involved in the data transaction flow in a face-to-face POS payment transaction in a full EMV environment.

### 4.1. Point-of-Sale Transaction Authorization and Data Transaction Flow in different Payment card Environment

The magnetic stripe environment existed prior to the introduction of the EMV smartcards for banking transactions. In this old system, the manuscript signature (i.e. the cardholder's signature) was the sole means of authentication, legality and authorization at the Point-of-Sale (POS) terminal by the customer. In other words, during the POS transaction, the cashier through visual inspection tries to authenticate the signature of the cardholder by comparing it to the one at the back of the payment card and also by checking for physical features such as the hologram. The magnetic-stripe transaction process starts when the cardholder swipes the card for payment through a magnetic reader; while the transaction is being processed, the cashier does a visual inspection of the card, requires the cardholder signature on the transaction receipt and then compares the name, number and the signature on the card to those on the transaction receipt [10],[11].

The hybrid transaction process starts when the cardholder swipes the card for payment through a magnetic reader, or dips the card into a chip-reading device. If the cardholder swipes the magnetic stripe of the card on the card reader, the merchant enters the transaction amount and the cardholder enters the PIN and a transaction authorization request is transmitted to the acquirer. The acquirer gateway or the back office electronically sends the authorization request to a third party (e.g. Visa) and other transactions are transmitted to the appropriate network. The third party then passes on the request to the card issuer. The card issuer does the necessary checks and also makes sure the cardholder has available funds before approving the transaction and providing an online response. The response is then forwarded by the third party to the acquirer, who then sends it to the merchant. The transaction is then completed when the merchant receives the authorization response [11]. On the other hand, if the cardholder is required to use the chip, the process begins when the cardholder dips the card into a chip-reading device; the terminal generates a list of applications supported by the card and the terminal, then the cardholder will be asked to select an application or the application will be

automatically selected, after the application is chosen then the terminal must select the application on the card, so that the card can supply correct data records for the transaction. Once the application is selected, the terminal provides the card with any data requested in the PDOL (Processing Options Data Object List) and gets the processing options. The Application Interface Profile (AIP) indicates the authentication option supported by the card and the terminal chooses the highest method supported by itself and the card. Next the terminal reads the application data records from the card which is made possible by the Application File Locator (AFL) supplied by the card. These records contain the card's PAN, expiry date and other information used for transaction processing like the card authentication and cardholder verification [2]. The EMV cards also contain a list of cardholder verification methods (CVM) they support, indicating the conditions under which they should be applied. For instance, the CVM list might contain when to use a signature, or a PIN, or to do nothing at all in order to verify the cardholder. The terminal must navigate through this list and attempt the options in the order predefined by the card issuer and the terminal may also skip an option that it is not capable of. This negotiation is performed between the card and the terminal, so as to establish what cardholder authentication method must be used. However, the vast majority of the transactions require the cardholder to enter the PIN on the PIN entry device. When the PIN is entered, it is sent to the card and the card compares it to the PIN stored in it so as to confirm that the cardholder knows the correct PIN and avoid fraudulent transaction and after a specified number of attempts if the PIN entered is wrong, the card locks up. If the PIN is correct the transaction proceeds to the next stage and the terminal requires the card to generate a cryptographic MAC over the transaction details, which is sent to the issuer (i.e. the bank that issued the card). This cryptogram includes a type code, sequence counter identifying the transaction, variable length field containing the data generated by the card and a MAC – calculated over the rest of the message including a description of the transaction. The MAC is computed using 3DES along with a symmetric key shared between the issuing bank and the card.

For a full EMV transaction, only the chip is used and the transaction process follows the same procedure as the latter stage described for the use of the chip in the hybrid environment.

### 4.2. The Payment Card Industry Data Security Standard Requirements Corresponding to the Cardholder Data Transaction Flow

The PCI DSS appears to be designed with magnetic stripe technology in mind since it emphasizes the protection of the cardholder data and sensitive authentication data anywhere the data is present in the transaction process which when exposed could lead to security breach and when taken advantage of by criminals will eventually lead to fraud [12]. PCI DSS is only applicable if the primary account number (PAN) is stored, processed, or transmitted [3]. The data elements of the cardholder include the PAN, cardholder name (which is not required to be transmitted) and expiration date. The mode of transaction of the cardholder data as regards to the magnetic-stripe, hybrid and the EMV environments differ in the processing and transmission phases of the cardholder data while the storage process remains the same in these three environments.

The DDA card mechanism is used to prevent card cloning and to authenticate the genuineness of the card but not the subsequent transactions performed by the card [12]. The DDA and the CDA cards are capable of performing dynamic data authentication while the SDA card can only perform static data authentication.

The unique feature of dynamic data authentication is that it prevents the transaction data from being fraudulently reused even if it was stolen from the processor's or merchant's database thereby making the data of little or no use to the criminal. This is because the transaction security and risk management considerations are such that all defenses are required to be at equal levels as much as possible so as to bring the PCI DSS in line with the threat landscape that exists in a full EM environment. Also since PCI DSS represents a minimum set of control objectives [13], it is not proper that the control should be excessive than required otherwise it creates an imbalance in the allocation of resources. Table 2 shows the PCI DSS requirements and the phase(s) that corresponds with each requirement in relation to the data transaction flow during any transaction. It is important to bring to mind that in a full EMV environment, the magnetic-stripe will be done away with but the iCVV will be present in the chip of the EMV smartcard. Therefore, as regards to the PCI DSS version 2.0, all the requirements that have to do with the magnetic-stripe will be aligned with a full EMV environment by the removal of references to the magnetic-stripe attached to the requirements. For some requirements that involve the storage, processing or transmission of the magnetic-stripe transaction mode interwoven in them, for instance the requirement 6 of the PCI DSS version 2.0, which makes reference to developing and maintaining secure systems and application, involves both the transmission and storage phases of the transaction, so the transmission phase will be adjusted and made to align with the EMV environment while leaving the storage phase to remain the same.

After critical examination of the PCI DSS version 2.0 as regards face-to-face transactions, it was discovered that there are no major changes to the standard except for the removal of the conditions that pertain to the magnetic- stripe features of the payment card, and the ranking of vulnerabilities defined in requirement 6.2 and 6.5.6 considered as best practice until June 30, 2012 which will become a requirement after that date [3]. One of the likely rationales for this is that, basically the PCI DSS was built around securing the PAN while that of a full EMV environment is centered on the use of unique symmetric key for the CDA card and asymmetric cryptography used by the card to digitally sign data to prove its authenticity to the terminal and the issuer thereby providing a greater level of fraud prevention compared to that of the magnetic stripe or the hybrid environment. Basically, it becomes more evident that with the EMV chip technology, the risk of compromised data being used for fraudulent transaction is significantly reduced. In other words, even if the data were to be compromised, the likelihood of being used to carry out fraudulent transaction is much reduced. However the PCI DSS still remain relevant in the hybrid environment according to [20] because some merchants and processors still accept non-EMV transactions prior to full migration to a full EMV environment. It therefore becomes evident that the PCI DSS is limited in preventing

attacks targeted specifically at unauthorized disclosure of cardholder data during a transaction because the EMV chip technology is designed to protect the cardholder data during a transaction with the implementation of the embedded chip in the payment card and a PIN to prevent abuse of lost or stolen card in a hybrid environment.

**Table 2. Table Showing the PCI DSS Requirements Corresponding to the Phases Involved in the Cardholder Data Transaction Flow during any Transaction.**

| Control Objectives (Goals) | PCI DSS Requirement | Transaction phase involved |
|---|---|---|
| Build and maintain a secure network | 1) Install and Maintain a firewall configuration to protect cardholder data | Transmission |
| | 2) Do not use vendor-supplied defaults for system passwords and other security parameters. | Processing and Transmission |
| Protect cardholder data | 3) Protect stored cardholder data | Storage |
| | 4) Encrypt transmission of cardholder data across open, public network | Transmission |
| Maintain a vulnerability management program | 5) Use and regularly update anti-virus software or programs | Processing |
| | 6) Develop and maintain secure systems and applications | Processing and Storage |
| Implement Strong Access Control Measures | 7) Restrict access to cardholder data by business need-to-know | Processing |
| | 8) Assign a unique ID to each person with computer access | Transmission and processing |
| | 9) Restrict physical access to cardholder data | Storage |
| Regular monitor and test networks | 10) Track and monitor all access to network resources and cardholder data | Processing |
| | 11) Regularly test security systems and processes | Transmission and processing |
| Maintain an information security policy | 12) Maintain a policy that addresses information security for all personnel | Storage, transmission and processing |

This in effect, makes the applicability of the PCI DSS in relation to a full EMV environment reduced. However, as relevant changes, improvements and new payment opportunities are being developed such as the implementation of the advanced authentication method provided by the CDA variant of the EMV payment card in a full EMV environment for POS terminal transactions and the use of robust authentication process for CNP transactions, the need to keep PAN and other sensitive data (such as the expiry date) confidential is significantly reduced while still allowing transmission of the PAN and other sensitive data in clear text at the POS terminal. Therefore, the PCI DSS will either become unnecessary since the PCI DSS is used as a control measure to make up for the vulnerabilities that exist in security of the payment transactions made in the hybrid environment otherwise, the PCI DSS would need to be updated in other to bring it in line with the threat landscape that would then exist in a full EMV transaction environment [20].

On the alternative, considering update of the PCI DSS in a full EMV environment may not also be necessary with the deployment of the enhanced authentication method provided by the CDA variant of the EMV card for POS terminal transactions and additional authentication data used for cardholder verification method during the CNP transactions in a full EMV environment.

In February 2011, Visa introduced the Technology Innovation Program (TIP) for its merchants outside of the United States in a bid to promote EMV chip technology in the United States and the same program will also be adopted and become effective in the United States by October 2012. One of its minimum criteria for the merchant qualification standard is that if a merchant can verify at least 75 percent of its transaction originates from an EMV transaction, then the requirement to validate compliance to the PCI DSS may be waived [12], [19], [20]. Note, this was proposed by Visa for merchants while still under the hybrid environment as an alternative to PCI DSS compliance. However, unless MasterCard, American Express, JCB International and Discover Financial Services launch similar EMV adoption programs, the merchants are still mandated to comply with the PCI DSS requirements annually while payment transactions are made in the hybrid environment.

## 5. Conclusion and Future Work

We have been able to show based on the survey on the known attacks against the payment card and consequences of unauthorized disclosure of cardholder data that the CDA cards will be the most desirable option if EMV becomes the sole means of payment in a face-to-face transaction, coupled with a globally robust authentication process for card-not-present (CNP) transactions and the need to keep the PAN and other sensitive authentication data confidential would be significantly reduced. We also showed how the implementation of a full EMV environment will impact the 12 requirements of the PCI DSS version 2.0 by analyzing the cardholder data flow during any transaction process. The future work of this research can be done in the area of implementation of a full EMV transaction using mobile phones for payment transaction due to the advancement and the increase use of smart phones worldwide for payment transaction such as direct mobile billing due to the significant progress made in the field of telecommunication.

## 6. Acknowledgement

The first author will like to thank the research team of Concordia University College of Alberta for their positive criticism, support and guidance in the completion of this research; his parents, siblings and Katherine W. Mitchell for their support and love throughout his studies and also his profound thanks to God Almighty for the gift of life.

## 7. References

[1] Douglas King, “Chip-and-PIN: Success and Challenges in Reducing Fraud” Retail Payments Risk Forum, January, 2012.[Online].Available:

www.frbatlanta.org/documents/rprf/rprf_pubs/120111_wp.pdf

[2] Ogundele Oludele, Zavarsky Pavol, Ruhl Ron and Lindskog Dale, "Implementation of a Full EMV Smartcard for a Point-of-Sale Transaction", World Congress on Internet Security (WorldCIS), 201, Publication Year: 2012, Pages(s): 28 – 35.

[3] Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 2.0, October 2010. [Online]. Available: https://www.pcisecuritystandards.org/security_standards/documents.php

[4] MasterCard, "Card Personalization Validation" [Online]. Available: http://www.paypass.com/CPV/CPV_Manual.pdf

[5] S. Balfe and K.G. Paterson, "e-EMV: Emulating EMV for Internet payments using Trusted Computing Technology", Information Security Group, Royal Holloway, University of London, UK. 2008. [Online]. Available: http://www.isg.rhul.ac.uk/~kp/EEMV.pdf

[6] S. J. Murdoch, S. Drimer, R. Anderson, and M. Bond, "Chip and Pin is Broken "IEEE Symposium on Security and Privacy, p 433-446, 2010, 2010 IEEE Symposium on Security and Privacy, SP 2010. pp. 433 – 444. [Online]. Available: www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf

[7] EMV – Integrated Circuit Specifications for Payment Systems, Book 2: Security and Key Management, version 4.2 ed., LLC, June 2008.

[8] Omar S. Choudary, "The Smart Card Detective: a hand-held EMV interceptor", June, 2010. [Online]. Available: www.cl.cam.ac.uk/~osc22/docs/mphil_acs_osc22.pdf

[9] Ross Anderson, Mike Bond and Steven J. Murdoch. "Chip and Spin", March 2005. [Online]. Available: http://www.chipandspin.co.uk/spin.pdf

[10] Steve J. Murdoch, University of Cambridge Computer Laboratory, 2009 [Online]. Available: www.cl.cam.ac.uk/~sjm217/papers/deaeslr09reliability.pdf

[11] Keith E. Mayes and Konstantinos Markantonaiks, "Smart cards for Banking and Finance" in Smart cards, tokens, security and applications, New York: Springer Science Business Media, LLC. NY, 2008, pp. 120 -125.

[12] Joeri de Riuter and Erik Poll, Formal Analysis of EMV Protocol Suite, Digital Security Group, Radboud University Nijimegen, Netherlands. 2011 [Online] Available: http://www.cs.ru.nl/E.Poll/papers/emv.pdf

[13] Saar Drimer, Steven Murdoch and Ross Anderson, "Failures of Tamper-Proofing in PIN Entry Devices" in IEEE Security and Privacy v 7 no 6 (Nov- Dec 09), pp. 39 - 45. [Online]. Available: www.cl.cam.ac.uk/~sjm217/papers/ieeesp09tamper.pdf

[14] Drimer, S., Murdoch, S.J. and Anderson, R." Optimised to Fail: Card readers for online banking". In: Dingledine, R., Golle, P. (eds.) FC 2009. LNCS, vol. 5628, pp. 184–200. Springer, Heidelberg (2009) [Online]. Available: www.cl.cam.ac.uk/~sjm217/papers/fc09optimised.pdf

[15] Toni Merschen, Fraud dynamics in the card payments industry: A globalreview of the realities of EMV deployment, In: Journal of Payments strategy & systems, Bd. 4 (2010), 2, S.156-169. January, 2010.

[16] Card Acceptance Guidelines for Visa Merchants, 2011. [Online]. Available: http://usa.visa.com/download/merchants/card-acceptance- guidelines-for-visa-merchants.pdf

[17] Visa Introduces Technology Innovation Program for Merchant, Visa Bulletin. 9 February, 2011. [Online]. Available: usa.visa.com/download/merchants/bulletin-tip-020911.pdf

[18] PCI Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard [Online]. Available: https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf

[19] Dr. H. Mark, "The Impact of EMV Conversion on Payment System", 2011. [Online]. Available: http://www.transactionworld.net/articles/2011/october/security.asp

[20] Visa Expands Technology Innovation Program for U.S. Merchants to Adopt Dual Interface Terminals. [Online]. Available: http://usa.visa.com/download/merchants/bulletin-tip- us-merchants-080911.pdf