Using Credit/Debit Card Dynamic Soft Descriptor as Fraud Prevention System for Merchant

Roy Laurens
Department of Computer Science
University of Central Florida
Orlando, FL, USA
rlaurens@knights.ucf.edu

Cliff C. Zou
Department of Computer Science
University of Central Florida
Orlando, FL, USA
czou@cs.ucf.edu

***Abstract*—This paper presents a novel method of using Dynamic Soft Descriptor as a fraud prevention method for Merchant (as opposed to card Issuer) in a credit/debit card transaction under Card Not Present (CNP) environment, such as online transactions. A unique identifier is embedded into the transaction descriptor, which will instantly appear in the cardholder's credit/debit card online statement. By checking his online statement, or calling his credit/debit card bank, a cardholder can obtain this identifier; and then provides the Merchant with this identifier as a proof of access to the statement. As the identifier is propagated using card association's back-end system and as only legitimate cardholder can access the card's statement, it is very unlikely that a fraudster can obtain this identifier information. Unlike other fraud prevention proposals, this proposed method is readily available and can be used right now by Merchant without the need for explicit support from card Issuer. Furthermore, it can be used starting with the very first transaction. So, it is more attractive than ordinary fraud detection method that requires significant amount of transactions. It can be readily deployed under the current card processing infrastructure, and we will show real life result at an e-commerce Merchant.**

Keywords—Electronic Commerce; credit card fraud; Card Not Present; dynamic soft descriptor; fraud prevention; chargeback

I. INTRODUCTION

The Internet revolutionizes commerce by enabling the existence of virtual markets. It allows Merchants to only have virtual existence and allows customers to conduct worldwide market transactions without leaving their homes [1]. The whole customer experience with online purchases can now take just a couple of seconds – from seeing an advertisement for a product to delivery of the item.

Currently, the primary method of payment for online transactions is **cards**, which include both debit and credit cards [2]. Allowing real-time authorization, this payment method has broad customer penetration and mature infrastructure in place. This real-time authorization feature is especially important for **Digital Merchants** (i.e., Merchants with digital/non-physical products such as software, digital videos and music), as it allows instant gratification that their customers usually seek.

Unfortunately, the attractive features of universality, ease and speed of online transactions using cards are also making cards very susceptible to fraud. In U.S., for example, 45% of total card fraud is from **CNP** (Card Not Present) payments, which include online payments [3].

Many fraud issues in online transactions are caused by the absence of physical card. Traditional anti-fraud method that works well with physical storefront – such as using hard-to-duplicate chip to obtain card information, or user ID (such as driver license) verification – cannot be used in online transactions. This makes it very difficult for Merchants to verify that an authorized cardholder is the one performing the online transaction. Therefore, under the rule of **payment card association** brands, such as Visa and MasterCard, online Merchants usually will be held liable if a cardholder later disputes the online transaction – a process known as **chargeback**. Because of this liability burden, Merchants have great incentive to prevent or reduce card fraud.

On the other hand, online transaction allows usage of fraud prevention tools that are uncommon or difficult to use in physical storefront. Some examples include: Address Verification System (AVS), Card Verification Value (CVV), and 3D-Secure (3DS) [4]. Some tools – such as 3DS – are actually quite complicated and require separate provider and infrastructure. But online Merchants need to utilize every available security tools, as ultimately they are the one that will be penalized for any fraudulent transaction submission.

Another incentive for Merchants to reduce card fraud is the threat of suspension from card association if their chargeback rate is above certain threshold. Even if a Merchant can absorb the financial cost of fraud in order to optimize its monetary gain [5], the card association might revoke the Merchant's account, which means it cannot accept cards as payment anymore. This will be catastrophic for online Merchants as card is still the primary method of payment for online transactions.

Ultimately, a Merchant's ability to combat fraud is very limited compared to its Acquirer (the entity processing the card transaction on Merchant's behalf) or card Issuer (the bank that issues the credit/debit card) because it can only observe its own card transactions. The Issuer and Acquirer, on the other hand, are able to detect pattern over a much larger transaction volume, which makes it easier for them to detect fraud [6]. However, they are more reluctant to decline a transaction or mark it as fraudulent because they do not want to cause inconveniences to their customers. This puts Merchant somewhat at a

disadvantage: it is liable for fraud yet its monitoring/tracking capability is much more limited compared to Issuer and Acquirer.

In this paper, we present a novel fraud prevention system that can be used by online Merchants. It is achieved by using the **Dynamic Soft Descriptor** feature [7] to provide strong confirmation of whether or not an authorized cardholder conducts the online transaction. During the authorization process, a unique identifier will be embedded in the transaction descriptor. This identifier will be propagated through the card back-end processing system, and it will be displayed on cardholder's card statement. The cardholder will then obtain this unique identifier from his/her card Issuer (via phone or online statement) and verify this unique identifier with the Merchant as proof that he/she has the access to the statement, and therefore is the authorized cardholder. The proposed fraud prevent system can be readily deployed under the current card processing infrastructure, and has been tried out successfully by a real online Merchant.

The structure of the paper is as follows: In next section we provide brief introduction to card transaction processing. Next, Section III provides more in-depth review of various tools to combat fraudulent card usage. In Section IV we formulate the problem of developing ideal fraud prevention system for online transactions and show the detail of our system. In Section V we show the real-life result as implemented by an online Merchant. We will discuss some improvements and limitations in Section VI. Finally, Section VII concludes the paper.

II. CARD TRANSACTION PROCESSING

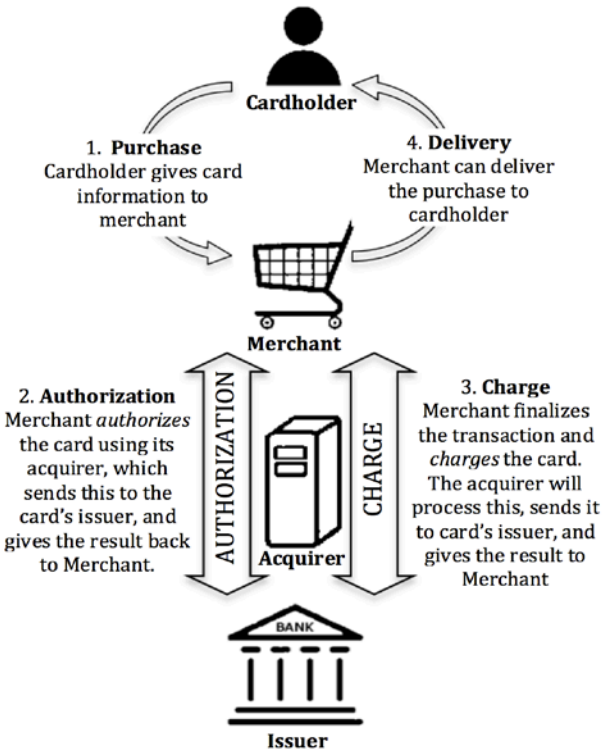


Fig. 1. Online Card Transaction Processing

Because the paper focuses on reducing fraud for online Merchants, we only introduce online transaction processing in this section.

1) Purchase: A cardholder makes a purchase at a Merchant's website and provides his/her card information. The Merchant usually will also ask additional information, such as shipping/billing address, phone number, CVV code, etc. Some fraud prevention and detection methods are deployed here as well, such as gathering IP address, device fingerprinting, etc.

2) Authorization: Merchant submits card authorization request to its Acquirer. Any Merchant that wants to accept cards has to open a Merchant Account at an Acquirer – which usually is also the Merchant's bank. For example, a Merchant that is a customer of Bank of America can use Bank of America Merchant Services (BAMS) as his/her Acquirer.

Authorization request contains the Merchant's information, cardholder's card information and information about the transaction, such as amount, type of transaction (i.e., telephone or Internet). Most of the time, the communication between Merchant and Acquirer is conducted via *payment gateway*, for example First Data/Payeezy or Authorize.Net.

Based on the card information, the request will be routed via the card association's back-end system to the card's *Issuer*, which is usually a bank. The Issuer will then respond with a decision whether to approve this authorization or not. This response will also contain results of the various fraud prevention checks, such as the AVS and CVV.

The Merchant receives authorization response from its Acquirer and continues processing of the transaction. If the authorization is denied, then Merchant can contact the buyer and ask for alternative payment. If authorization is approved, Merchant can perform further fraud detection checks and decides whether to continue processing.

3) Charge: If Merchant decides to continue the transaction, it sends a *charge* request to the Acquirer. Merchant should not charge the card until the goods that the buyer wants to purchase is available and ready to be delivered.

4) Delivery: If the charge is successful, Merchant will start the shipping process and deliver the item to the buyer.

III. RELATED WORK

In general, Merchant's method to combat fraudulent card usage can be categorized into two groups: tools to *prevent* fraud and tools to *detect* fraud.

A. Fraud Prevention Tools

These tools are used to prevent card fraud by asking the buyer for additional information to help verify the cardholder's identity at the time of purchase [4]. Below are some of the most common industry-standard tools for online transactions:

1) Address Verification System (AVS): AVS is a system used to verify the address of cardholder by checking the billing address of the card provided by the buyer with the address on file at Issuer. During authorization, AVS is used when the Merchant verifies card data, such as billing address and ZIP

code, against the Visa/MasterCard billing information of the cardholder.

AVS only verifies the numeric portions of a cardholder's billing address. For example, if the address is 101 Main Street, Highland, CA 92346, in the United States, AVS will check *101* and *92346*.

For online Merchants, AVS is not very useful as most fraudster that has access to stolen card information usually also has access to its billing address. The Merchant usually will perform some transaction review if shipping address and billing address is different. However, this cannot be utilized by digital Merchant, which sends its product via email.

2) Card Verification Value (CVV): CVV is an additional code/number in the card that is not part of the card number. In VISA/MasterCard, it is a three-digit code printed in the back of the card, which is different than the card number that is printed in front. During authorization, CVV is sent to the Issuer, which can verify it against the CVV it has on file.

Unlike card number, Merchant is not allowed to store CVV code, and it has to be asked from the cardholder for every different transactions. This will reduce the probability that a data breach will expose the CVV.

Although CVV is a better predictor of fraud compared to AVS, it still suffers from the same basic flaw: card fraudsters usually have access to CVV as well.

3) 3D-Secure (3DS): The basic concept of 3DS is to prevent fraud by allowing Issuer to verify customer at the online point of purchase [8]. VISA implementation of 3DS is called Verified by VISA, whereas MasterCard implementation of 3DS is called MasterCard SecureCode. One beneficial feature of 3DS for Merchant is it *shift the liability* of fraud from Merchant to card Issuer.

A transaction at Merchant that has 3DS will initiate a redirection to the website of the Issuer to authorize the transaction. Each Issuer could use any kind of authentication method (the protocol does not cover this) but typically, a password-based method is used, so to do Internet purchase, buyer has to use a password tied to the card.

3DS is very attractive to online Merchant, due to its liability shift feature. However, 3DS depends on Issuer's support, and a lot of Issuer simply does not support it [9]. Furthermore, customer experience with browser redirection and additional Internet password has been very poor. Hence, Merchant might lose more money due to bad customer experience than to chargeback.

4) Out-of-Band Verification using phone: Merchant can use the phone number provided when the buyer makes a purchase as a verification tools by sending a text message (if it is a mobile phone) [10] or automated voice calls [11]. The buyer would then confirm this message back to the Merchant to authenticate the transaction.

However, this method's security depends entirely on phone number provided by the buyer. Unlike bank or card Issuer, Merchant does not have access to the cardholder's profile, and therefore cannot verify if the phone number provided is the same phone number associated with the card. Fraudster could easily give their own phone number, which makes this tool practically useless.

Some researchers propose using a combination of mobile phone and cellular-based solution to develop a framework for authenticating transaction [12], or live authentication of cardholder using telephone banking [13], or even new card transaction framework [14]. But all these approaches depend on Acquirer and card Issuer's cooperation in building and maintaining a new infrastructure. Considering the fact that even industry standard such as 3DS is still not universally supported, it will take an even longer time for new proposals to be supported.

B. Fraud Detection Tools

Whereas fraud prevention tools is designed to prevent fraudster from completing the transaction successfully, fraud detection tools will try to calculate the possibility that a completed transaction is fraudulent and, if necessary, perform additional review on it.

Fraud detection works by analyzing several different attributes of the transaction, such as the amount, location, velocity (number of orders made by the same cardholder), IP geolocation, etc., and assigning a risk factor/value to these attributes. These attributes and values are fed into detection system which will analyze them and mark the transaction as fraud if necessary.

There is a considerable research in fraud detection, which uses various methods such as neural network [15], behavioral analysis [16], and other techniques [17,18]. Unfortunately, all these methods require a significant amount of transactions before they can accurately detect fraudulent transaction. This makes them less useful for Merchant, which only has a limited number of transactions to analyze. Furthermore, since Issuers are working with a large volume of transactions, they can absorb fraud loss more readily than Merchant. A fraud detection method that will identify fraudulent transaction after ten such transactions might be acceptable to Issuer, but it could be financially infeasible for Merchant.

Therefore, although all Merchants must utilize fraud detection as part of their overall anti-fraud strategy, more emphasis should be put into fraud prevention system.

IV. PROPOSED APPROACH: DYNAMIC SOFT DESCRIPTOR BASED SYSTEM

As discussed in previous section, an ideal fraud prevention system for online Merchant will need to have the following characteristics:

- **Low friction**: In the end, Merchant wants to maximize legitimate transactions. The system should not create difficulties for legitimate buyers.
- **Fast turnaround**: Transaction verification should be conducted near real-time, as most buyers want instant gratification.

- **Use available infrastructure**: Individual Merchant has no control over its Acquirer and card Issuer. So, Merchant can only utilize available methods and process.
- **Universal**: Online transactions are conducted worldwide, with numerous Acquirer and Issuer. Ideally, the system should be compatible with all Acquirer and Issuer so that all online transactions can be verified.
- **Low Cost**: A lot of online transactions, especially for digital goods, involve a very small amount of money. Ideally, the system should be free.
- **Automated**: An automated system will be able to handle fluctuations in transaction volume.

A. *Dynamic Soft Descriptor*

A *descriptor* is a piece of identifying information about a Merchant, e.g. business name, phone number, city and/or state, which appears on buyers' card statements. These descriptors provide cardholders with the detailed information of purchases and give them a way to identify and contact the Merchant if necessary. The standard descriptor information that gets passed through to the cardholder's statement is the name and customer service phone number that a Merchant provided when it opens its Merchant account with its Acquirer. As this descriptor is static, all purchases made at the same Merchant will generally show up as the same text in every cardholder's statement.

However, most Acquirers, such as Paypal [19], First Data [20], and Bank of America [21], also support *dynamic soft descriptors*. This is a seldom used feature that allows Merchant's transaction descriptor to be modified on a per-transaction basis. Merchant with multiple locations might add the location name, or other transaction-specific information into the descriptor text. For example, the cardholder statement will show "STARBUCKS MAGIC KINGDOM FL" instead of just "STARBUCKS".

Currently, the role of soft descriptor in fraud prevention is practically non-existent, as it is just used to minimize *friendly chargeback*, which happens when a legitimate transaction is disputed by the cardholder because the person does not recognize the transaction. The additional per-transaction message offered by soft descriptor should be able to provide better information to help reduce such misunderstanding – especially since some cardholders could receive their statements a month after the transaction. In contrast, we propose using this soft descriptor as part of fraud prevention system by utilizing it as a separate and secure communication channel from Merchant to its cardholder.

B. *Dynamic Soft Descriptor as Fraud Prevention System*

As the soft descriptor message is independent and transaction-specific, we can use this as a channel for *out-of-band authentication*. In this case, we will use it in a way similar to multi-factor authentication because it utilizes a separate communication channel, namely the authorization process between the Merchant, the Acquirer and the Issuer, until it is displayed in cardholder's card statement.

Out-of-band authentication is an old concept and it is already used in financial institutions and other organizations with high security requirements, some of which use SMS/text message on mobile phones [22]. The practice makes hacking an account more difficult because two separate and unconnected authentication channels would have to be compromised for an attacker to gain access. In the same way, utilizing soft descriptor as online transaction verification makes using fraudulent card more difficult because fraudster would have to compromise both the cardholder's card information and his/her access to the card's online statement in order to successfully pass the fraud prevention system.

The steps for performing fraud prevention system using soft descriptor are outlined below:

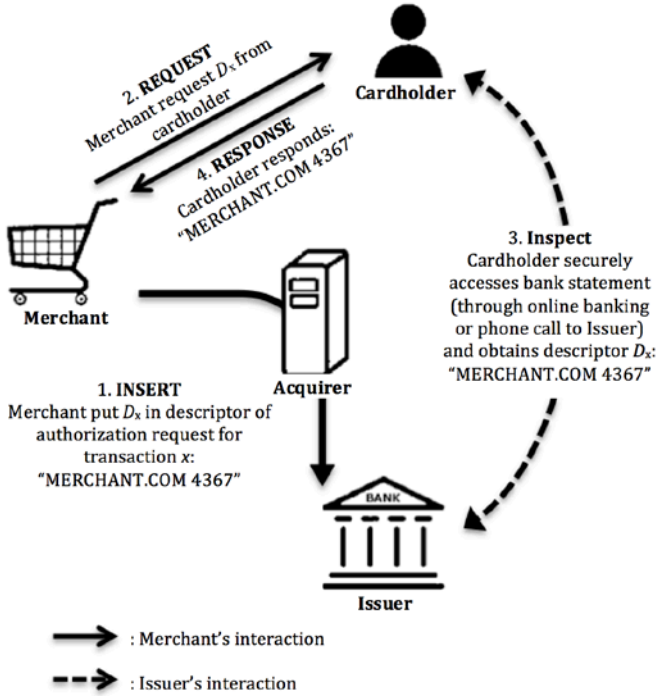


Fig. 2. Dynamic Soft Descriptor Authentication Steps. Merchant inserts unique descriptor which will be verified by cardholder via card statement.

1) Insert: Merchant embeds a randomly chosen unique identifier (D_x) in its soft descriptor as part of its authorization request for transaction x. As normal part of authorization, the Acquirer will propagate D_x to Issuer, and Issuer will show it in cardholder's statement. It should be noted that it is the card Issuer's discretion as to how many characters will show up in the cardholder's statement [20]. But in general, a descriptor of 22 characters or less should show up in its entirety. As an example, if Merchant is using First Data and D_x is '4367', the message will be in JSON (JavaScript Object Notation, a lightweight data-interchange format) as follows [23]:

```
{
  "gateway_id": "A00001-01",
  "password": "zzzz",
  "transaction_type": "00",
  "amount": 11,
  "cardholder_name": "JEFFREY LEBOWSKI",
  "cc_number": "4111111111111111",
  "cc_expiry": "0314",
  "soft_descriptor": {
        "dba_name": "MERCHANT.COM 4367"}
 }
```

2) Request: Merchant requests a cardholder to provide the descriptor text about this transaction in his/her bank statement. The request can be sent selectively (i.e., only for high-risk transaction) via email, or it can be displayed on the webpage at the conclusion of checkout and payment.

3) Inspect: Cardholder has to access the bank statement in order to obtain descriptor for this transaction, which contains D_x. Access to cardholder's account is usually governed by a high level of security that is commonly used by financial institutions, such as card Issuer. Therefore, Merchant is indirectly utilizing the Issuer's security protocol to protect D_x and only makes it available to authorized cardholder. In cardholder's statement, the transaction descriptor usually contain additional text, such as date, amount, authorization number, etc. For example, the soft descriptor JSON data on step 1 might show up as follows:

05/04/2015 Merchant.com 4367 139241 $13.76

4) Response: Cardholder provides transaction descriptor to Merchant as proof that he/she has access to bank statement. If this is authentic, Merchant should be able to find D_x as part of the descriptor. As only authorized cardholder has access to the statement, Merchant can assume that the transaction is not a fraud and authorized by the cardholder.

C. Security Analysis

This Soft Descriptor Fraud Prevention System depends on the assumption that only authorized cardholder is able to access the statement that contains Merchant's transaction-specific unique identifier. We believe this assumption is well warranted as most data breaches compromise either card information or online credentials, but never both. For example, Target data breach [24] exposes its customers' card information, but not the online access to those cards, as this information is not known to Target. Likewise, Citibank's 2011 account hacking compromises their customers' accounts, but not the card's CVV code as this information is not stored in the account [25]. This is probably because card information and account access are usually resided in separate systems. When cardholders log into their Issuer's system, they cannot see their card's full information, such as CVV. In other words, card fraudsters usually don't have login information of the online profile associated with the card, and vice versa: hackers that breached online bank accounts usually don't have full card information.

Moreover, the unique identifier is propagated using card Processor's back end system, which is totally separate from the Merchant's website, and even from card Issuer's own customer-facing systems. So, fraudster that wants to defraud a Merchant will need to gain access to that Merchant's back end processing system, or the Merchant's Processor. These are much more complicated than the common data breach associated with card fraud.

This system also meets the requirements of ideal fraud prevention system outlined earlier, namely:

- **Low friction**: Merchant can selectively request the descriptor only on high-risk transactions, thus there is no extra burden for known buyers, such as verified customers. Therefore, any degradation in customer experience can be targetted towards a select high-risk transactions. Admittedly, it can be argued that there are some inconveniences for accessing card statement. But since the transaction is already conducted online, it should not be a big hassle for the buyer to also perform online statement access.
- **Fast turnaround**: As will be shown in the next testing section, the descriptor usually shows up practically instantly in the card statement. So, the turnaround time will mostly depend on how fast the statement can be accessed – which entirely depends on the cardholder.
- **Use available infrastructure**: Dynamic Soft Descriptor is a standard feature that is already available at some of the largest card Acquirers [19,20,21]. It can readily be deployed because it does not require any further cooperation from Acquirers or Issuers.
- **Universal**: As a descriptor is essential in identifying the transaction in cardholder's statement, support for soft descriptor is universal. In the next section we will show descriptor output from various card Issuers around the world.
- **Low Cost**: There is no extra charge in using soft descriptor compared to static one. By default, however, it is usually not enabled. In that case, Merchant needs to request its Acquirer to enable this feature.
- **Automated**: Although the system explained in this paper is using manual verification, it can easily be automated using a simple script. For example, Merchant can create a simple transaction authentication webpage, where a customer can enter his/her transaction ID and the description as it is shown in his/her card statement. Then, Merchant can authenticate the identifier using simple php script such as this:

```
// transaction's unique descriptor
$descriptor = '4367';

// user-provided statement
$userstmt =
  '05/04/2015 .com 4367 139241 $13.76';

if (strpos($userstmt, $descriptor) === false) {
  // fail
} else {
  // pass
}
```

V. Real-Life Testing Results

We are able to secure the cooperation of an e-commerce Merchant that has both US and international customers to deploy the system presented in this paper. As this is a production environment, we are processing real transactions with real credit/debit cards.

A. Propagation time

We measure the amount of time it takes from Merchant's authorization request containing D_x until it shows up in the statement as 'pending' transaction. This is done by submitting a

transaction while continuously reloading the online statement on the card Issuer's website. For completeness, we do this on three of the largest card Issuers in USA and we try different combination of VISA/MasterCard and Credit/Debit card.

We perform this measurement test with our own real credit/debit cards, and therefore has to limit the testing to only five trials per card. Otherwise, the excessive card usage might trigger fraud warning on Acquirer of the Merchant's account, and all transactions might be suspended.

TABLE I. PROPAGATION TIME

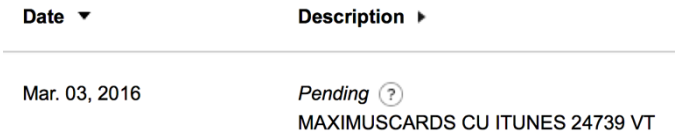
Card Issuer	*Avg Time*
Citibank MasterCard credit	< 1 second
Bank of America VISA debit	75 seconds
Chase Bank VISA credit	< 1 second

The results are shown in Table I. As expected, the identifier shows up instantaneously, except for Bank of America debit card. We think this is because the debit card is not an actual standalone payment card but an access tool to the checking account. The delay might be due to Issuer's internal process of settlement between the card and its checking account. A workaround for this issue is presented in section VI.

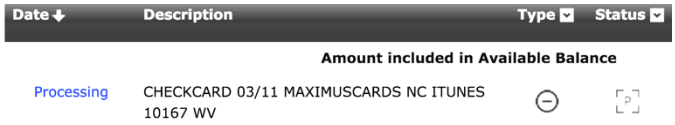
B. Sample Card Statement

Due to space constraint of soft descriptor [20], the online Merchant that utilizes this system is using 2 random alphanumeric character as D_x. These are the screenshot of the various payment card's online statement:

1) Citibank MasterCard credit: The D_x used is 'CU', and the Merchant inserts it in the middle of its real transaction description, so the full descriptor becomes 'MAXIMUSCARDS CU ITUNES'. This is shown in the Citibank's online statement as follows:

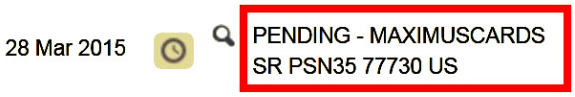


2) Bank of America VISA debit card: The D_x used is 'NC', and the full descriptor becomes 'MAXIMUSCARDS NC ITUNES'. This is shown in the Bank of America's online statement as follows:



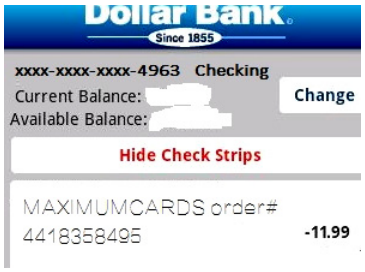
3) Chase Bank VISA credit card: The D_x used is 'FJ', and the full descriptor becomes 'MAXIMUSCARDS FJ XBOX3M'. This is shown in the Chase Bank's online statement as follows:

4) Commonwealth Bank Visa credit: Soft descriptor support should work on international cards as well. In this case, we use Commonwealth Bank, which is a prominent Australian Bank. The D_x used is 'SR', and the full descriptor becomes 'MAXIMUSCARDS SR PSN35'. This is shown in the Commonwealth Bank's online statement as follows:



5) Qatar International Islamic Bank VISA credit: Qatar International Islamic Bank is another large international credit card Issuer based in Doha, Qatar – which is a country in the Persian Gulf. The D_x used is '4Z', and the full descriptor becomes 'MAXIMUSCARDS 4Z ITUNES'. In this case, the customer took a picture of the statement from his screen and forwarded it to the Merchant. Although the statement is mostly in arabic, we can clearly see the desriptor in the middle.

6) Fraud Attempt: During the real-life trial of our system on the collaborated Merchant, we have actually caught some frauds successfully. The following screenshot shows a failed attempt by a fraudster trying to fake the statement. The bank name and logo can be obtained easily because the first six digit of card number indentifies the Issuer. However, fraudster cannot obtain the real statement and instead has to guess the contents of the description, which clearly failed.



VI. DISCUSSION

Although this system is designed for online Merchant, it can easily be adapted to other CNP scenarios, particularly the Mail-Order/Telephone-Order (MOTO) transactions. Instead of online access, a cardholder's bank statement can be accessed via telephone call to the Issuer's customer support number.

This system should also be able to reduce friendly chargeback, which usually happens when the payment card is borrowed and used by someone close to the cardholder. It might be common for people sharing the same household to borrow one another's card, but it is much less likely that the person borrowing the card will know the cardholder's online access credential.

One issue reported by the Merchant running this system is that some Issuers cannot provide real time access to the statement. A similar issue is when there is a significant propagation delay, as in the case of Bank of America VISA Debit. In these cases, one workaround is to take the risk and process the transaction, but block subsequent purchases from the same card until the first transaction is verified. In this way, at most the Merchant will suffer the financial loss of one transaction.

Another reported issue is the complaint that some customers have due to the inconvenience of accessing their online statement. This can be remedied by educating the customers, providing alternative (such as calling the Issuer), or even offering incentives (such as offering 5% discount or gift certificate to a customer when he or she is put through this verification process). As a matter of fact, some customers do express their support of this authentication method, as it is considered less intrusive than asking for a copy of ID card or driver license.

In addition, a Merchant can activate the proposed fraud prevention system only when a transaction is suspicious (measured by other fraud detection systems). In this way, utilizing the proposed fraud prevent system will not add much burden to most customers of a Merchant.

Finally, as mentioned in Section 1, a Merchant's primary incentive to reduce fraud is the threat of suspension from card association if their fraud rate is above certain threshold. This suspension could put the Merchant in Terminated Merchant File (TMF) or MasterCard Alert to Control High-risk Merchants (MATCH) list [26], which makes it practically impossible for the Merchant to open a new account with any credit card processor.

VII. Conclusion

In this paper we show how we can use an existing Soft Descriptor feature in card transaction to prevent fraud by embedding a unique identifier into the descriptor. The detection relies on the fact that the real cardholder has access to his or her credit/debit card statement (via online banking or phone call to the bank), while the fraudster does not. We also provide real life data on an online Merchant that uses this system. The output from several major card Issuers is presented. Finally, we also show a real incident by a card fraudster trying to cheat the system but failed.

VIII. Acknowledgement

This work is supported by the Seed grant from Florida Center for Cybersecurity (FC2).

References

[1] Yaser Ahangari Nanehkaran, "An Introduction To Electronic Commerce", International Journal of Scientific & Technology Research Volume 2, Issue 4, April 2013.

[2] TSYS, "2014 Consumer Payments Study", October 2014.

[3] Julie Conroy, "Card Not Present (CNP) Fraud in a Post-EMV Environment", Aite Group, June 2014.

[4] VISA, "Card-Not-Present Security: A Multi-layered Approach to Payment Card Security", www.visa.ca, December 2010.

[5] A. C. Bahnsen; A. Stojanovic; D. Aouada; B. Ottersten, "Cost Sensitive Credit Card Fraud Detection Using Bayes Minimum Risk", Machine Learning and Applications (ICMLA), 2013.

[6] C. Whitrow, D. Hand, P. Juszczak, D. Weston, and N. M. Adams, "Transaction aggregation as a strategy for credit card fraud detection," Data Mining and Knowledge Discovery, vol. 18, no. 1, pp. 30–55, Jul. 2008.

[7] Michael Ross, "Dynamic Soft Descriptors", Payeezy Gateway, support.payeezy.com, February 2016.

[8] MasterCard, "Advancing Security in Internet Transactions", 2010.

[9] Susan Pandy, "Mitigating Fraud Risk in the Card-Not-Present Environment", Federal Reserve Bank of Boston, February 2016.

[10] W. Yan and D. Chiu, "Enhancing E-Commerce Processes with Alerts and Web Services: A Case Study on Online Credit Card Payment Notification", In Proceedings of the International Conference on Machine Learning and Cybernetics, 2007.

[11] CDYNE Corporation, http://cdyne.com/api/phone/notify/, 2016.

[12] Frank S. Park, Chinmay Gangakhedkar, Patrick Traynor, "Leveraging Cellular Infrastructure to Improve Fraud Prevention", Computer Security Applications Conference, 2009.

[13] H. Xiao, B. Christianson, and Y. Zhang, "A purchase protocol with live cardholder authentication for online credit card payment", 4th International Conference on Information Assurance and Security (IAS), 2008.

[14] S. Gupta, R. Johari, "A New Framework for Credit Card Transactions Involving Mutual Authentication between Cardholder and Merchant", Communication Systems and Network Technologies (CSNT), 2011.

[15] S. Ghosh, D. L. Reilly, "Credit card fraud detection with a neural-network", System Sciences, 1994.

[16] Y. Zhang, F. You, H. Liu, "Behavior-Based Credit Card Fraud Detecting Model", INC, IMS and IDC, 2009.

[17] Y. Sahin; E. Duman, "Detecting credit card fraud by ANN and logistic regression", Innovations in Intelligent Systems and Applications (INISTA), 2011.

[18] M. R. HaratiNik, M. Akrami, S. Khadivi, M. Shajari, "FUZZGY: A hybrid model for credit card fraud detection", Telecommunications (IST), 2012.

[19] Paypal, Inc., https://developer.paypal.com/docs/classic/release-notes/Merchant/PayPal_Merchant_API_Release_Notes_115/, 2015.

[20] First Data Merchant Services, https://support.payeezy.com/hc/en-us/articles/203730599-Dynamic-Soft-Descriptors, 2015.

[21] Bank of America Merchant Services, Inc., https://merch.bankofamerica.com/global-gateway-e4-features, 2015.

[22] U. Onwudebelu; O. Longe; S. Fasola; N. C. Obi; O. B. Alaba, "Real Time SMS-Based hashing scheme for securing financial transactions on ATM systems", Adaptive Science and Technology (ICAST), 2011.

[23] First Data Merchant Services, https://support.payeezy.com/hc/en-us/articles/204029989-First-Data-Payeezy-Gateway-Web-Service-API-Reference-Guide-#4.5, 2015.

[24] N. Eric Weiss, Rena S. Miller, "The Target and Other Financial Data Breaches: Frequently Asked Questions", Congressional Research Service, February 2015.

[25] Robert McMillan, "Citigroup hackers made $2.7 million", http://www.computerworld.com/article/2509496/security0/citigroup-hackers-made--2-7-million.html, 2011.

[26] MasterCard, "MATCH", https://developer.mastercard.com/documentation/match/ , 2016.