AN EMV MIGRATION FORUM WHITE PAPER

Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud

Version 2.0

Date: July 2016

EMV Migration Forum
191 Clarksville Rd.
Princeton Junction, NJ 08550

www.emv-connection.com

About the EMV Migration Forum

The EMV Migration Forum is a cross-industry body focused on supporting an alignment of the EMV implementation steps required for payment networks, issuers, processors, merchants, and consumers to ensure a successful move from magnetic stripe technology to more secure EMV contact and contactless technology in the United States. The focus of the Forum is to address topics that require some level of industry cooperation and/or coordination to migrate successfully to EMV technology in the United States. For more information on the EMV Migration Forum, please visit http://www.emv-connection.com/emv-migration-forum/.

TABLE OF CONTENTS

1 Introduction[1]

EMV chip migration in other countries shows that as EMV technology is implemented for card-present or face-to-face transactions in the United States, fraud will "shift to other types of card payments with weaker authentication protocols"[2] including card-not-present (CNP)[3] payments—Internet, mail order and telephone order—sometimes referred to as IMOTO. These transactions "will become a weak link in the defenses against fraud, and IMOTO fraud will likely increase." [2]

The U.K. experience supports this prediction. The move to EMV payments in the U.K. left IMOTO authentication unchanged. IMOTO fraud grew rapidly from the start of EMV deployment in 2003 until it peaked in 2008. Beginning in 2008, IMOTO fraud declined for several years as merchants implemented a more secure authentication protocol for Internet transactions (3-D Secure) and as magnetic stripe-only locations in continental Europe decreased, thus reducing the opportunity to use counterfeit magnetic stripe cards.[2] Data from the U.K., France and Australia[4] show that CNP fraud became a larger portion of overall fraud during and after their EMV chip conversions, as EMV chip dramatically reduced the card-present fraud issues but did not address the card-not-present fraud problem.

Spain took a different approach to card-not-present fraud during its migration to EMV technology. The difference between Spain's experience and the U.K.'s experience was described in a TSYS white paper.[5] The charts below illustrate the impacts from different approaches and priorities for mitigating fraud, depicting the complexity of the problem and the need for a comprehensive, sustained effort to combat it.

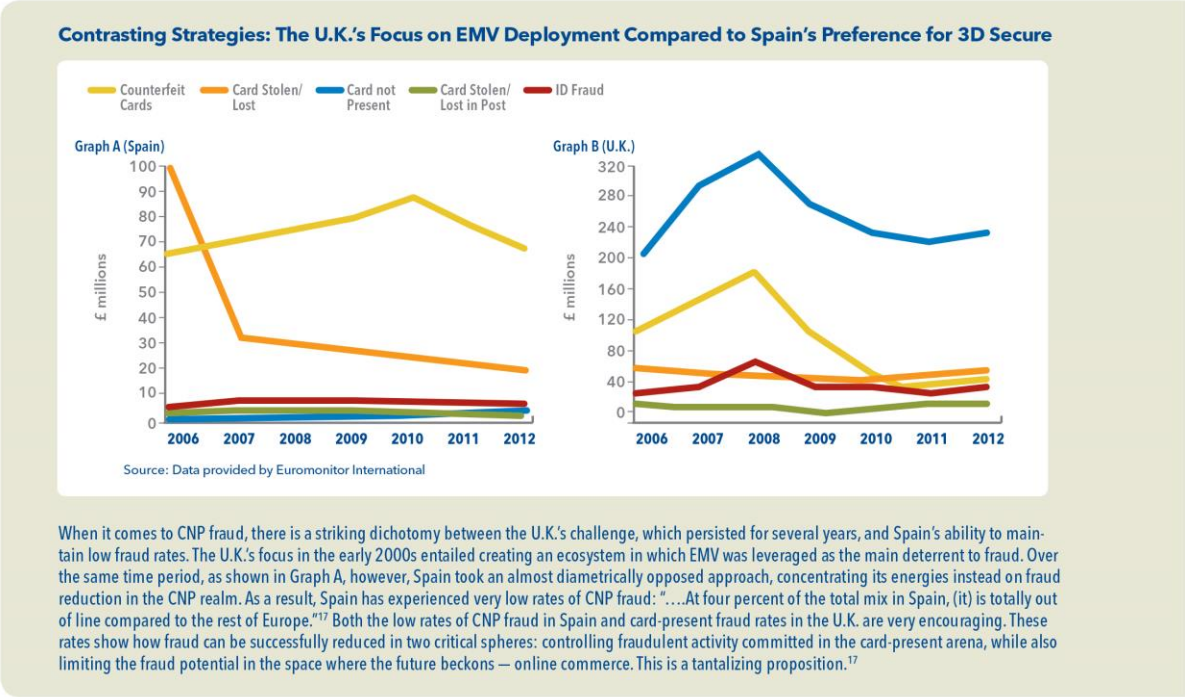


Figure 1. The U.K.'s Focus on EMV Deployment vs. Spain's Preference for 3D Secure.[5, 6]
(Note: For footnote 17 mentioned in the text of Figure 1, see footnote 4)

[1] Version 2.0 of the white paper adds Appendix B and Appendix C.
[2] "The U.S. Adoption of Computer-Chip Payment Cards: Implications for Payment Fraud," Richard J. Sullivan, Federal Reserve Bank of Kansas City's First Quarter 2013 Economic Review
[3] Appendix B includes payment industry definitions of CNP, related industry terms and acronyms, as well as some high-level use cases.
[4] "Card-Not-Present Fraud: A Primer on Trends and Authentication Processes," Smart Card Alliance, February 2014
[5] "EMV is Not Enough: Considerations for Implementing 3D Secure," TSYS white paper, by Jonathan D. Hancock, 2013, http://www.tsys.com/Assets/TSYS/downloads/wp_emv-is-not-enough.pdf
[6] "Evolution of Card Fraud in Europe 2011-2012." *Fico.com*. Web. November 2013, http://www.fico.com/landing/fraudeurope/Evolution_Europe.html

This white paper describes best-practice recommendations for using authentication methods and fraud tools to secure the CNP channel. The paper focuses primarily on CNP e-commerce transactions.[7]

Accordingly, the paper provides information from which a merchant can construct CNP security solutions, based on one or more methods, to strengthen its system against various vulnerabilities and better protect its system from attacks and fraud. Integration of multiple methods, for example layered in combination with one another, ensures a merchant's system has stronger security than any one method alone can provide.

While the paper addresses many techniques applicable to e-commerce transactions that originate from desktop computers, tablets, laptops and mobile phones, it does not specifically address the emerging mobile payments environment.

To identify best practices for mitigating CNP fraud, the EMV Migration Forum Card-Not-Present Fraud Working Committee (the "Committee") evaluated the current viable authentication methods and fraud tools, using 27 measurable parameters. The Committee considered these parameters to be key factors in determining the effectiveness and success of a method or tool. They included, for example, user friendliness, learning curve, convenience, and strength of security. Each authentication method or fraud tool assessed was assigned a score for each parameter. The parameter scores were then totaled, providing an overall score for each method or tool. This process was intended to help ensure objectivity, provide an audit trail for decision-making, and maximize input and participation.

A total of 14 authentication methods were identified and evaluated. Key stakeholder groups – composed of merchants/acquirers, issuers and payment networks – performed the initial evaluation. Using the same evaluation criteria, these stakeholder groups then met independently to identify each group's three to five top methods. The groups then met together as the full Committee to identify the top five authentication methods overall.

A similar process was followed to evaluate the fraud tools. The Committee first compiled an inventory of fraud tools, consulting both subject matter experts and the CyberSource "2013 Online Fraud Report."[8] The individual stakeholder groups then evaluated the fraud tools independently. Finally, the groups met together to review their findings and discuss effectiveness, ease of integration with the authentication methods, and impact on abandonment rates.

For each authentication method and fraud tool, this paper summarizes the impact on the affected stakeholder groups of cardholders, merchants, card issuers, and acquirers. In this way, this paper seeks to provide a commercial understanding about how each method operates and what elements of fraud protection may be afforded.

Once this exercise was completed, it became clear to the Committee there is no "silver bullet," and the best practice for CNP fraud mitigation is a multi-layered approach—rather than identifying a single best tool, identifying a basket of authentication methods and fraud tools that work together for a successful fraud reduction program is a best practice recommendation.

Industry, technology and criminal behavior are evolving rapidly, and therefore it is critical industry stakeholders make a concerted effort to stay informed about the viability of both current and new techniques as they emerge.

[7] Because some of the authentication methods and fraud tools discussed may not be applicable to the CNP mail order or telephone order (MOTO) environments, where appropriate, discussion of a specific method or tool indicates whether that method or tool can be used in a MOTO environment.

[8] "2013 Online Fraud Report," CyberSource, Online Payment Fraud Trends, Merchant Practices, and Benchmarks, 14th Annual Addition. (The page link cannot be provided as it is only accessible/downloadable with a member login.)

2 Authentication Methods

Identity authentication for a card-not-present transaction – one that is requested by a consumer not present at the retail merchant location – is defined as the process of ensuring that the owner of the account being used to pay for the purchase is performing the transaction. Identity authentication in this context typically relies on a person providing one or more of the following *authentication* factors:

- Something the person has, such as a credit card (*ownership* factor).
- Something the person knows, such as a PIN (*knowledge* factor).
- Something the person is or does, such as a fingerprint (*inherence* factor).

Experts often recommend authentication processes that require at least two factors and ideally all three factors (multifactor *authentication*). Relying on a single factor implies either extremely high confidence or extremely high tolerance for risk.

This section examines the following authentication methods, which were identified as the best practice authentication methods:

- Device authentication
- One-time password
- Randomized PIN pad
- Biometric factors

Each section includes the potential impact of a method on different stakeholders.

2.1 Device Authentication

Device authentication, deployed primarily by financial institutions and e-commerce merchants, authenticates the device being used to access the merchant's e-commerce site (e.g., smart device, personal computer or tablet). The method authenticates the device based on multiple device characteristics (e.g., device type, operating system, IP address) acquired either before or during a transaction. Defining the exact characteristics that identify an individual device can be complicated. The identification software can be homegrown or purchased from a third party. Multiple services are available from third-party providers. Companies that track the successful and fraudulent transactions associated with the devices can assist in their authentication.

Because this method authenticates the device and not the cardholder, additional authentication is required to protect against the use of lost or stolen cards. Device authentication does not address mail order or telephone order (MOTO) transactions.

2.1.1 Impact on Consumers

Device authentication is designed to run in the background when visiting a merchant's website. The consumer is usually not aware of the process unless the device is not recognized.

Another consideration is that one of the characteristics often used for device authentication is the device's IP address. (Note that many different characteristics can be used.) Given that some Internet providers use dynamic addresses by default, the use of dynamic IP addresses may interfere with the method's ability to accurately recognize a device.

While the requirement for consumer interaction is minimal, if the device is not recognized, the consumer may be prompted to enter answers to one or more security questions (or respond to other challenge/response dialogs). And because consumers often use different devices to access the Internet at different times, the consumer experience may depend on what device is being used. Cardholders who use public computers (e.g., in a public library or in an Internet cafe) may be affected more than those who regularly use their own devices.

Since device authentication runs in the background and identifies a consumer's specific device, privacy concerns are sometimes raised with this method.

2.1.2 Impact on Merchants

Merchants have the largest stake in device authentication. The e-commerce messaging standards currently used by many payment networks cannot pass device authentication parameters from a merchant to an issuer for issuer evaluation. However, standards for updated messaging are being developed both within the United States and internationally and new standards are underway that will impact this area. Until those standards become commonly implemented, a process which could take years, merchants must either partner with a fraud prevention vendor or build their own device identification capabilities in-house.

Implementing device authentication with a new vendor may involve significant cost and workload. Cost and workload can also be significant if the merchant builds the process in-house. Development and implementation can include both software and hardware costs. An additional disadvantage is that an in-house solution might not have as much volume of data or different types of data as a vendor-based solution.

Typically, merchants with many repeat customers, implying established relationships, benefit the most from using device authentication. Merchants with lower numbers of repeat customers, however, may be able to use vendor-provided industry-aggregated data to benefit from this authentication tool.

2.1.3 Impact on Issuers

Most card issuers have implemented device authentication on their consumer banking web sites. When the device authentication system does not recognize the consumer's device, the consumer may be required to provide additional information. Using a third party can provide access to industry-aggregated data, allowing issuers to recognize devices consumers have not used previously to connect to the issuer's web site. Traditionally, card issuers do not use device authentication data in authenticating a CNP transaction because generally payment industry messaging standards (versions of ISO/IEC 8583) cannot pass device authentication parameters from the merchant to the issuer.

2.1.4 Impact on Acquirers

Acquirers can act as service providers for smaller merchants to implement device authentication. In this case, the impact on the acquirer is similar to the impact on a merchant.

2.1.5 Other Considerations

In combination with other authentication techniques, device authentication can reduce the risk of fraudulent transactions. One potential complication is that different providers may use different characteristics to define devices.

When device authentication is used alone, privacy considerations are minimal. The data are used only to mitigate merchant risk, and the information is technical (e.g., IP address) rather than personal (e.g., name, email address, phone number). However, as an article in the August 2014 issue of *IEEE Spectrum*[9] describes, there can be some privacy concerns when device authentication data is combined with proprietary or other validation data (Section 3.1 and Section 3.2).

2.2 One-Time Password

A one-time password (OTP) is a password that is only valid once. Since OTPs are dynamic and cannot be reused, their use can prevent replay attacks. Additionally, OTPs are often implemented to be time sensitive, either because they are generated during a valid transaction or because they are time-synchronized with the entity that

[9] "*Browse at Your Own Risk,*" Nick Nikiforakis and Günes Acar, August 2014, North American: Spectrum.IEEE.org.

generates them. Unlike other tools, OTPs can feasibly be used in all CNP channels: Internet, telephone, and mail order.

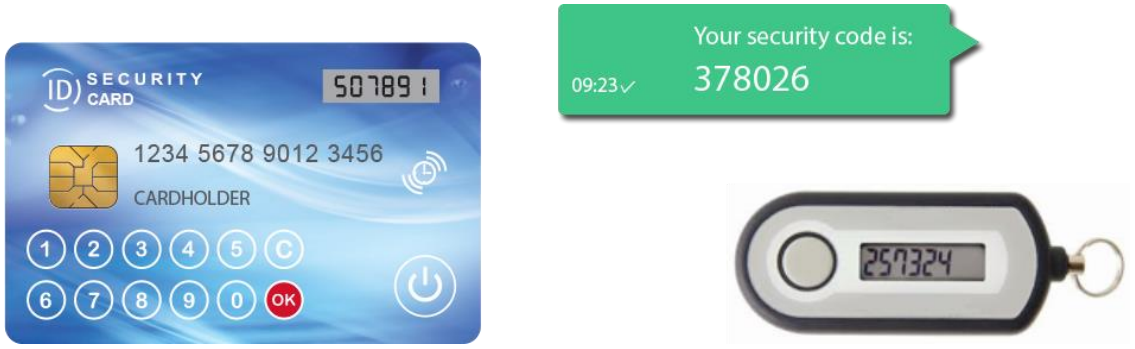
A method is required to deliver OTPs to users. Common delivery methods include hard or soft tokens, display cards, text messaging, and Internet-based channels. Delivery is also possible using paper or other physical media (e.g., scratch cards) in countries where electronic delivery methods are not practical. If the delivery method is out of band from the transaction being performed, OTPs can be an effective component of two-factor authentication.

Methods for generating OTPs include random generation, mathematical algorithms, and time-synchronized algorithms. The method chosen for OTP generation and delivery directly affects and increases the strength of OTP as an authentication solution. The following three solutions reflect stronger authentication:

- Truly random generation and one-way algorithms since the OTP cannot be reverse engineered.
- Integrating OTP with other methods since the OTP by itself is susceptible to "man in the middle" and phishing attacks.
- Reducing the timeframe when an OTP is valid.

OTPs must be paired with user IDs or card numbers, and security is often layered with a static password, PIN, or pass phrase.

Figure 2. Example of OTP delivery; from left to right: display card integrating payment function and OTP generator, SMS OTP, discrete OTP token



2.2.1 Impact on Consumers

Because OTP requires consumer involvement, it is less convenient than a passive authentication method. Consideration should therefore be given to using OTP as part of a layered approach and only requiring the OTP in high-risk situations.

Some OTP solutions require the consumer to have a device that can generate or receive the OTP, which may require additional consumer education and training. Also, some OTP delivery methods, such as SMS text messaging, require the consumer to opt-in and may incur a usage charge (e.g., a mobile operator text messaging fee). One way to eliminate the need to carry two separate devices is by using display cards, which integrate a screen and a keypad in the same card.

2.2.2 Impact on Merchants

Typically, an issuer generates and delivers the OTP. The merchant must therefore allow for OTP input in the transaction stream. Since the use of OTPs requires the consumer to take an additional step, OTPs may increase the risk of consumer abandonment before checkout.

If the merchant chooses to generate and use OTPs then the merchant must account for the cost of the solution and provide for customer enrollment. When the OTP is delivered out-of-band, the merchant will need to verify the consumer's contact information.

2.2.3 Impact on Issuers

Use of OTPs increases both the number of steps and the time required to authenticate a CNP transaction. As a result, both the risk of transaction abandonment and the potential that the consumer will use a different payment method also increase. The issuer should therefore consider integrating OTP with a risk-based authorization method, such as device authentication or a risk-based approach using 3-D Secure (3DS) or similar technology (see Appendix: Terms and Definitions). The issuer can then define the risk threshold at which an OTP is required.

When issuers are responsible for managing the OTP solution, as is generally the case, they must evaluate the different generation and delivery methods. Such methods may require in-house infrastructure and software development or licensing with a third party to manage the process. If the OTP is delivered using a hard token, issuers will have to replace lost and expired tokens. Soft-token delivery methods and out-of-band methods may incur lower replacement costs.

Issuers also need to address how to integrate the OTP process into the transaction authorization stream. They may need to adjust their current authorization rules and processes.

Lastly, some level of consumer education is required. Consumers must be made aware that they will receive an OTP, how it will be delivered, and how to use it to reduce consumer friction or abandonment.

2.2.4 Impact on Acquirers

Use of OTPs has no effect on acquirers. However, acquirers can act as service providers for smaller merchants to implement OTP. In this case, the impact on the acquirer is similar to the impact on a merchant.

2.2.5 Other Considerations

If a display card feature is added to an EMV chip card, the card manufacturer will need to have the card certified and approved in the same fashion as a standard EMV chip card. Adding this feature to a card without a PIN pad nullifies the protection OTP offers against the use of lost or stolen cards, since the fraudster can supply the OTP being generated on the card.

Use of an existing mobile device to generate or receive an OTP obviates the need to obtain and carry an additional device, display card or token to generate or receive OTPs. These solutions, although serving similar purposes, have a wide range of cost considerations, driving some stakeholders to favor one particular method over another.

2.3 Randomized PIN Pad

The randomized PIN pad authentication method allows consumers to enter a PIN to complete a transaction and use their PIN-enabled debit or credit card for e-commerce purchases. This method can also be used for one-time PINs, as described in the previous section and for credit card POS PINs, as described below. When consumers indicate they want to pay using a card from a bank that contracted for this method, a PIN pad floats on top of the e-commerce merchant's checkout page (Figure 3).

Figure 3. Example of a Virtual PIN Pad

The consumer uses their pointing device (a mouse or their finger for a touch screen) to enter a PIN (thus preventing key logging). After each mouse click, the keypad is scrambled, and only the XY coordinates of each click are captured. When the PIN and other card data have been entered, the customer submits the transaction. The XY coordinates that represent the PIN are encrypted and sent to a data center, where they are converted to PIN characters and encrypted according to industry standards in a hardware security module (HSM). The PIN is never in the clear or stored at the merchant location.

PIN data-request details are combined with the other authorization data to form an ISO/IEC standard 8583 message, which is sent to the issuer for authorization. The authorization response message is then returned to the merchant from the issuer's authorization system.

Many merchants currently use a randomized PIN pad to authenticate e-commerce transactions. Consumers in the U.S. can use PIN-enabled debit cards to make e-commerce purchases without having to register on the merchant's web site (and enter data such as a user name or password) or leave the site.

Credit cards with PINs used at the point of sale can also use the random PIN pad for Internet purchases. Some chip-enabled credit cards in the U.S. may require the use of a PIN at the POS. Typically, magnetic stripe-only credit cards in the U.S. do not, although a PIN is required to obtain cash from an ATM. As some U.S. credit cards become chip and PIN enabled, beginning in 2015, they will be eligible for using the random PIN pad solution, assuming their issuers support the feature.

The same randomized PIN pad process can be implemented for PCs, laptops, tablets, and phones, thus standardizing the payment process across many different platforms. The randomized PIN pad can be used for both static PINs and one-time use PINs. Randomized PIN solutions are supported by various issuers, processors and merchants across the U.S.

2.3.1 Impact on Consumers

The randomized PIN pad offers a way to authenticate consumers directly on a merchant's checkout page. The consumer should be aware the keypad is scrambled after each click and not to enter their PIN too quickly.

The industry has trained cardholders to be vigilant and to use their PINs in as private a manner as possible. The same cardholders have adopted this service, when supported by their issuer and the merchant, with very little education.

2.3.2 Impact on Merchants

Merchants can implement randomized PIN pad authentication by working with their acquirer and can usually be operational within a short time.

Randomized PIN pad authentication provides an additional layer of authentication, requiring the consumer to have both their card number and their bank-issued PIN. This reduces the number of chargebacks and the number of fraudulent transactions.

According to the February 2009 Identity Fraud Survey Report by the Javelin Research Group[10], $21 billion in online sales are lost each year due to consumer security concerns. Since consumers are already familiar with using PIN pads for debit and ATM transactions, they tend to adopt this method of online security readily. In addition, the randomized PIN pad can be integrated into the merchant's e-commerce checkout page, keeping consumers on that page and reducing cart abandonment rates.

The web site instructs consumers to use the mouse to enter the PIN and notifies them that the keypad will scramble after each number is selected.

[10] "2009 Identity Fraud Survey Report (Full Version)," Javelin Strategy & Research, February 2009, https://www.javelinstrategy.com/brochure/114

2.3.3 Impact on Issuers

Randomized PIN pad authentication leverages existing systems and many POS networks in the U.S. and other countries to provide an additional level of security for e-commerce transactions. The critical issue is following industry-agreed PIN standards. Where that can occur, it typically requires no additional issuer IT resources, software or hardware purchases, or implementation. Issuers can design randomized PIN pads as an image of the consumer's card so that it looks familiar to the cardholder.

According to CyberSource's 2010 Online Fraud Survey Report,[11] 16.5 percent of e-commerce transactions rely on debit-style non-bank providers. However, this same survey showed that 63 percent of respondents would prefer to use a version of randomized PIN pad over a non-bank provider. Issuers adopting randomized PIN pad authentication can capture these transactions and keep them in the issuing bank, thus maintaining income and transaction volumes.

2.3.4 Impact on Acquirers

Randomized PIN pad has also been implemented by acquirers in countries where EMV has been the card standard for some time, including India and China. There is some software integration work (limited development and testing) for acquirers who today do not support the service. However, the work is not significant and can be accomplished in a relatively short period.

2.3.5 Other Considerations

The randomized PIN pad solution was designed to address e-commerce security issues and capture debit transactions for both merchants and issuers. However, the approach may also support other types of PIN-enabled cards, including prepaid cards and credit cards.

2.4 Biometrics

While biometric authentication can be implemented across many types of consumer devices, this section is focused on implementations that authenticate a cardholder from a smartphone during a CNP transaction. Now that digital cameras have become a core feature of most smartphones, these devices can be used, in conjunction with required software, to perform facial recognition alongside voice recognition of a cardholder during a CNP transaction. Fingerprint scanners are also now available in a number of smartphones and can be used to authenticate a cardholder during a CNP transaction. Facial and voice recognition solutions typically perform their verification with a secure database server while fingerprint scanners that are embedded in smartphones typically perform verification in a secure location directly on the device.

Use of biometrics to authenticate a CNP transaction offers benefits and challenges. One benefit is increased reliability of identity authentication. The challenges depend on the type of biometric used and the channel through which it is implemented. While a promising technology, use of biometrics raises both privacy and liability concerns. Given the sensitive nature of biometric data, the data should usually be transmitted out-of-band unless a very secure in-band transmission technique is available.

Not all types of biometrics may be appropriate for use with all CNP transactions, and implementers may wish to consider related factors such as implementation costs, reliability and user friendliness.

Smart devices can authenticate consumers in-band, using a mobile app on the phone to perform the transaction, or out of band, when another device is being used. Out-of-band e-commerce biometric authentication protects against most known attacks, such as man-in-the-browser (and its variations). Information describing the transaction can be shown on the smart device screen before the transaction is completed. If the displayed transaction information does not match the actual transaction, the consumer is able to decline the transaction.

[11] "Online Fraud Report," 11th Annual Edition, February 2010, CyberSource, (the page link cannot be provided as it is only accessible/downloadable with a member login)

2.4.1 Impact on Consumers

Using biometrics for authentication is convenient for most consumers. In addition, using the smart device for biometric authentication increases the potential for immediate acceptance.

When a smart device is used to acquire the required biometric data, there is very little learning curve for the consumer. The consumer can download an application and enroll over the phone. Smart devices include a camera (which can capture a picture of the consumer's face) and a microphone (which can capture the consumer's voice); these devices support multiple forms of authentication, and enrolling by taking a picture or creating a voice recording is simple.

When consumers perform a CNP transaction using a smart device, the merchant's (or mobile payment app host's) app automatically requires authentication at checkout (as described in the following section). Consumers use the smart device to perform the required face or voice authentication, either in band (if they are using the phone for the transaction) or out of band (if they are using a different device).

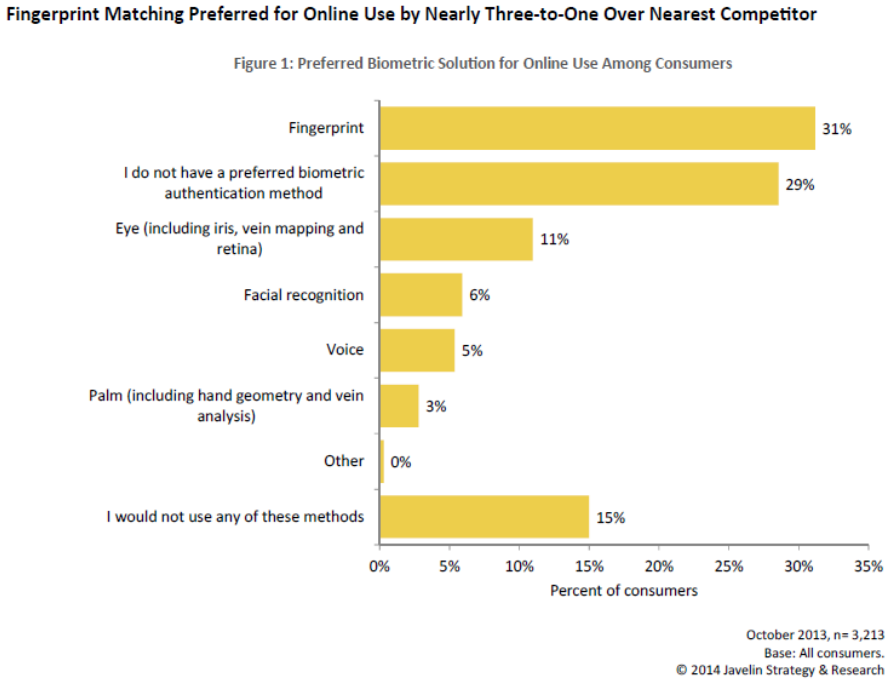
Consumer concerns about biometric authentication include issues such as how user friendly it is, where their sensitive information is stored, what security is provided for the storage location, and whether the biometric factor can be stolen and used for fraudulent purposes. **Error! Reference source not found.** provides a perspective from consumers on preferred biometric authentication methods.

2.4.2 Impact on Merchants

The simplest way for merchants to implement biometrics is to use 3-D Secure (3DS) or similar technology. Merchants do not need to know a biometric authentication is being performed.

To incorporate biometric authentication into the checkout process, merchants integrate a solution that performs biometric checking into their web site and enroll their customers. The process is similar to the process performed by an issuer to implement this solution. However, unlike the issuer, the merchant may not already have a relationship with the customer. As a result, guaranteeing identity reliability during the enrollment process may pose challenges.

Figure 4. Preferred Biometric Factors[12]



[12] "Biometrics in Banking and Payments," Javelin Strategy & Research, January 2014, www.javelinstrategy.com

2.4.3 Impact on Issuers

The most critical requirement for issuers is the enrollment process. Issuers must verify the identity of the consumer at enrollment. If issuers offer voice or face recognition through 3DS or similar technology, implementation may also require an authentication server and an app for the consumer's phone.

Consumer verification is straightforward if the consumer is a bank customer and enrollment is conducted at a bank branch. Typically, however, consumers do not want to go to a bank to enroll. In addition, many consumers may not have a checking account or other relationship with the card issuer; they may only have the issuer's credit card. In these cases, issuers must use an external authentication factor to enroll the consumer, such as a temporary PIN/passcode sent by mail.

The issuer implementation process does not require interaction with merchants, acquirers, or smart device manufacturers, assuming the merchants and acquirers already support 3DS or a similar process. If the biometric information will be stored in the secure element in the phone, issuers must interact with a mobile network operator or other entities controlling the secure element to implement biometric authentication.

2.4.4 Impact on Acquirers

The impact on acquirers implementing biometric authentication solutions using 3DS is discussed in Section 4. If the solution is implemented without requiring access to the issuer, the acquirer will not need to pass or process any biometric information.

2.4.5 Other Considerations

Biometrics cannot be shared or easily copied. The mobile application can be protected with a PIN/passcode to increase security, although requiring it may reduce the user friendliness of the solution.

An optional secure element (SIM card, micro SD, or embedded secure element) or trusted execution environment in the smart device, managed by a trusted service manager, can further protect the biometric data and application.

3 Fraud Tools

The evaluation process used by the Committee and described in Section 1 identified two best-practice fraud reduction tools:

- Proprietary data/transactional data
- Validation services

3.1 Proprietary Data/Transactional Data

Proprietary and transactional data can be collected by merchants, issuers, and acquirers and used to enhance risk management and fraud prevention activities. Proprietary data, defined as data owned by a single organization (merchant, issuer, or acquirer), has proven to be invaluable in identifying fraudulent payments. An example of proprietary data used in this way is a list of high-risk payment cards, e-mail addresses, IP addresses, and similar information, which is accrued over time by a merchant (i.e., a customer history). Transactional data is data collected at payment, either explicitly (e.g., name, ship-to address) or implicitly (e.g., web connection details). These data elements are specific to a single transaction.

3.1.1 Description

Before a merchant delivers a product or service, the associated payment-transaction data (e.g., buyer, payment method, endpoint/device, web connection, order details) can be analyzed to determine whether the transaction is likely to be fraudulent. This data can be gathered in a number of ways: scripts on a merchant's payment page, the browser or native mobile app request from the customer, proprietary intelligence collected over time, and order-related information provided by customers themselves.

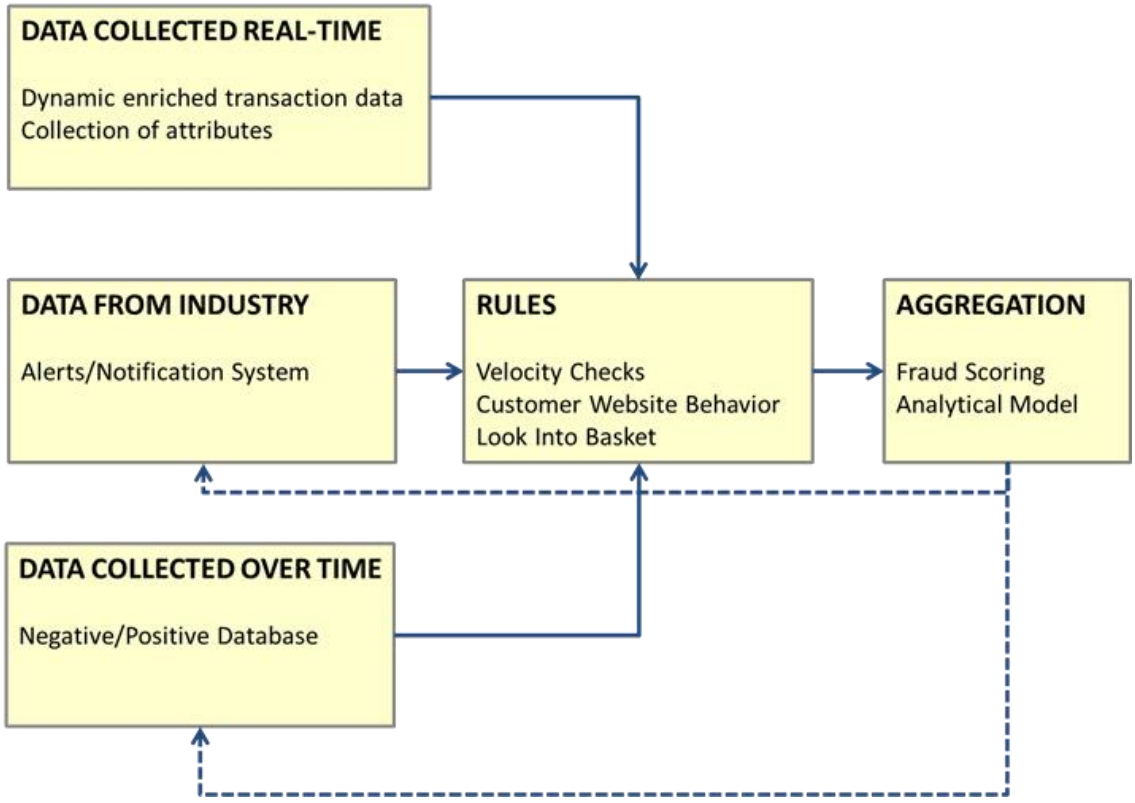
Once the customer completes a purchase, data collection is the first step in the risk management process (Figure 5). The data are either collected in real time (transactional data) or accessed as needed (proprietary data). All transaction details must be securely logged. Next, a rules engine that incorporates industry or homegrown fraud tools (such as velocity checks and dynamic order linking) analyzes the data, applying the rules or parameters defined by the decision maker. The results of this analysis are then used to calculate a fraud score, which is returned to a decision maker (merchant or acquirer) who can choose to approve or decline the transaction. When an authorization request is received, a card issuer can use similar data (although typically not endpoint device data) to develop its own score and authorization decision.

The types of data used to calculate a fraud score are determined by the type of risk being evaluated. Some examples are device attributes, web connection attributes, payment details, buyer information, order form attributes, and proprietary history. The fraud prevention model can be further enhanced through leveraging shared industry data.

3.1.2 Impact on Consumers

The consumer is not required to provide any additional data, and therefore the solution is transparent to the consumer.

Figure 5. Proprietary/Transactional Data Fraud Tool



3.1.3 Impact on Merchants

Merchants may feel some effects, depending on which part of the payment chain implements this type of fraud strategy and what particular tools are chosen. Merchants who choose to implement the strategy will need a solution capable of collecting, securely logging, analyzing, scoring, and acting on proprietary/transactional data. Merchants can opt to build a solution themselves, obtain an available solution, or implement a hybrid approach. In all cases, the system needs to evaluate overall risk based on the merchant's defined risk management rules.

The impact of implementation on a merchant will be determined by the merchant's current infrastructure and how much integration is required.

3.1.4 Impact on Issuers

The impact on issuers is similar to the impact on merchants. The main difference is that issuers may implement a separate process for collecting and analyzing relevant data to approve or decline a transaction. Issuers will have a broader view (and thus more available data), as a result of seeing transactions that originate with multiple merchants and acquirers. However, the data they can leverage may be limited, given their place in the payment stream. For example, issuers may rely more heavily on proprietary data (such as customer history) as opposed to transactional data.

3.1.5 Impact on Acquirers

The impact on acquirers is similar to the impact on merchants. The main difference is that acquirers may implement a separate process for collecting and analyzing relevant data to approve or decline a transaction. Acquirers will have a broader view (and thus more available data) as a result of seeing transactions that originate with multiple merchants and issuers. Their involvement with and closer proximity to merchants in the payment stream may give them more flexibility than issuers in certain cases.

3.1.6 Other Considerations

A subset of the rules and data (e.g., device and web connection details) will be relevant only to e-commerce payments. Most of the data can be applied to physical POS payments as well as well mail order and telephone payments.

3.2 Validation Services

A validation service uses customer information other than a primary account number (PAN) to validate that the actual card account holder is participating in a transaction.

A number of validation services are available. Merchants can adopt a single service, using a single control checkpoint, or multiple services, as a layered control check, with the option of accepting transactions at any point to reduce consumer friction. Each control point offers an additional opportunity to help reduce fraud.

The two predominant validation services are the address verification service (AVS) and card security code (e.g., CVV2, CVC2, and CID). Other validation services which match additional data elements (e.g., e-mail address, phone number) may provide tighter fraud screening but often require additional costs and resources.

3.2.1 Address Verification Service

AVS requires that the purchaser enter the billing address on file for the card. The issuing bank generates one of the following response codes, based on the numeric portion of the address line 1 and the zip code data that are passed as part of the transaction:[13]

- Full match. Both address and zip code match the billing information on file with the issuer.
- Partial match. The address matches but the zip code does not, or vice versa.
- Complete mismatch. Neither the address nor the zip code match.
- AVS not supported by issuing bank.
- System/technical error.

The disadvantage of using AVS for transaction authentication is that the consumer must understand the differences between the billing, mailing, and shipping addresses, because the billing address is used most often for AVS matches. Additionally, it may be difficult to validate foreign cardholders, due to different postal code formats. Postal code formats might not be available in all markets.

3.2.2 Card Security Code Validation Service

Card security code validation requires the purchaser to enter the security code printed somewhere on the physical card, for example such as next to the signature panel. The code is an encrypted value determined by elements that include card attributes, such as card number and expiration date. The issuer has the encryption key and can decrypt the code and validate it during transaction authorization processing. This service verifies that the CNP transaction is being conducted by someone who is in possession of the card being used. Dynamic security code, or DCVC/DCVV is also coming into the market where a new security code is periodically and automatically generated instead of using a static security code that is usually printed on back of the card.

3.2.3 Impact on Consumers

Validation services offer consumers the security of knowing a transaction will not be authorized unless their preferred credentials are verified. AVS and card security code are convenient forms of validation services, and using both can significantly reduce fraud.

[13] Note that actual response values and codes from each issuing bank vary somewhat and may continue to evolve in line with payment network mandates.

The AVS validation process is transparent to the consumer unless the billing address does not match the cardholder's address on file with the issuer. The consumer should be advised about the importance of supplying an accurate billing address during the transaction.

Card security code validation is widely used and thus may be more familiar. A small number of consumers may not know how to locate the code on the card. This impact can easily be mitigated by illustrating where to find the value.

3.2.4 Impact on Merchants

Merchants, who are the primary stakeholders, can incorporate validation services as part of a consumer best-practice program. E-commerce merchants may need to set up a payment service model that passes appropriate data and returns a response that is consistent with the merchant's tolerance for risk.

Merchants using AVS can offer consumers an "enroll" option that captures the consumer's billing address. However, the merchant will also need to allow consumers to purchase without enrolling, and fraudsters will probably not enroll.

Merchants may also have to consider how to archive billing and shipping records. Consumer information and stored AVS values should be archived securely in accordance with the applicable compliance requirements. For security and privacy, information about multiple consumers at the same address should be kept separate. Additionally, merchants may consider using a flag that trips if the ship-to address differs from the billing address, since a different ship-to address can signal a risk for fraud. When a transaction is flagged for this reason, the merchant should assess the transaction further before order fulfillment, to approve or decline it based on the merchant's risk tolerance.

Merchants using card security code validation must not retain the code after authorization. The Payment Card Industry Data Security Standard (PCI DSS) prohibits storing this value, and it is very important that this code is not stored anywhere on merchant systems.

The merchant's purchase page may need an information link or picture to show the consumer how to locate the security code.

Merchants with both a brick-and-mortar and an e-commerce presence must also consider how to verify customers at in-store pickup. The success of the validation service relies on the merchant's verification procedures.

It should be noted that an issuer is always free to decline a transaction for other reasons. An issuer may also choose to authorize a transaction, even when validation fails. The responses for the validation services are transmitted in separate fields from the general authorization response; the merchant may then decide whether to complete the transaction based on the complete picture of issuer responses.

Other considerations relate to business terms. Merchants should work with their acquirers to understand the fees that are assessed and the financial benefits, if applicable.

3.2.5 Impact on Issuers

Many payment networks mandate that issuers support AVS and card security code validation. Issuers should be able to support multi-level validation with minimal impact. When using AVS, issuers may also need to stress to merchants the importance of educating customers to properly enter billing address data.

A validation service offers issuers an additional level of security whereby the transaction was authorized by the cardholder, decreasing the likelihood of CNP fraud for issuers.

In the case of a dynamic security code, issuers must apply minor back-end changes to be able to validate the code. The cost of these changes, in addition to the form factor, may vary by issuer.

3.2.6 Impact on Acquirers

Acquirers must be able to accept the relevant data values and exchange them with merchants and networks. Acquirers who process CNP transactions will probably already have this capability.

Full support of AVS may require that acquirers' software systems normalize the AVS responses from issuers so that merchants can receive the full benefit. Acquirers will also need to pay attention to issuer compliance requirements and payment network mandated rules.

4 3-D Secure[14]

3-D Secure (3DS), in its current version, is a secure communication protocol used to enable real-time cardholder authentication directly from the issuer during an e-commerce transaction. The payment networks have built proprietary products on top of this protocol. The authentication process is initiated by 3DS software resident on the merchant's or its service provider's system; the cardholder is authenticated by a 3DS component operated by the issuing bank or its service provider. Authentication requires the cardholder to communicate a secret that is shared with the bank or that otherwise meets the bank's requirements. The purchase transaction, enhanced with the authentication data, is then processed through the traditional payment systems (including authorization, clearing, and settlement).

3DS divides transactions into three domains:

1. The issuer domain encompasses the systems, functions, and relationships of the issuer and its cardholders.
2. The acquirer domain encompasses the functions of the acquirer and its merchants.
3. The interoperability domain encompasses the systems and functions that enable the issuer domain and the acquirer domain to interoperate and authenticate each other within participating payment systems.

3DS supports multiple authentication methods, including static passwords, OTPs, the use of a participating bank's online banking credentials, the use of an EMV chip card reader, and biometrics. It can also be deployed using either a standard model, in which every transaction is authenticated with 3DS, or a risk-based model, in which cardholders require authentication with 3DS only when risk characteristics for a transaction exceed a predetermined level.

4.1.1 Impact on Consumers

Because the authentication method is determined by the issuing bank, the consumer experience can vary widely. The learning curve for the consumer and any resident software requirements depend on the authentication policies, authentication method, and implementation selected by the issuing bank. Consumers may be required to enter anything from a simple static password to an OTP that is sent to the consumer's mobile device. The method chosen by the bank depends on the bank's authentication policies and the capabilities of the issuer's 3DS service provider.

Consumers are affected most, however, by the issuing bank's implementation model. If the bank uses the standard model, cardholders must enroll before using 3DS for a transaction. If the bank uses the risk-based model, the consumer will not even realize 3DS is involved for all but the riskiest transactions. The risk-based model reduces the requirement for enrollment but may not eliminate it altogether; cardholder enrollment may still be required for higher risk transactions.

3DS solutions are intended to work on multiple platforms and channels; vendor solutions vary, however, in how successfully they perform across different channels.

4.1.2 Impact on Merchants

To use 3DS, merchants are required to incorporate 3DS capabilities into their checkout and payment platforms. The merchants can then authenticate themselves to multiple entities within the ecosystem (e.g., each payment network's directory server) and process the resulting authentication messages. The impact on an individual merchant therefore depends on the merchant's current infrastructure and the level of integration required to process the 3DS data properly.

[14] Appendix C includes a comparison of 3-D Secure 1.0.2 and 3-D Secure 2.0

3DS vendors can provide merchants with a variety of implementation solutions. Such solutions range from stand-alone Merchant Plug-In (MPI) packages, which integrate into a merchant's payment and checkout systems, to comprehensive on-behalf-of services, which not only manage the integration between a merchant's current processes and 3DS functionality, but also provide case management and reporting.

Business impact on a merchant is harder to predict. Any merchant who supports 3DS or similar technology for a payment network automatically supports all issuers for that brand; however, merchants have no control over the authentication process or requirements of individual issuers. For example, Activation During Shopping (ADS), a cardholder registration method that was widely adopted by issuers at one time, resulted in problems for merchants concerned about longer checkout experiences for their e-commerce customers. While risk-based issuer implementations can help address this problem, they continue to require processes that online merchants do not control. Merchants in the U.S., however, may also benefit from chargeback protection because 3DS shifts the risk to the issuer.

4.1.3 Impact on Issuers

Like merchants, issuers will have to support the 3DS protocol, authenticate themselves to multiple entities within the ecosystem, and process the resulting authentication messages. How 3DS impacts an issuer is determined by the issuer's own risk and authentication policies, the issuer's current infrastructure, and the level of integration required.

Any issuer adopting a 3DS solution will have to educate their cardholders. An effective communications plan should include information about what the program is, what its objectives and benefits are, and most importantly, what the cardholder may be required to do or may experience at checkout. Issuers should also ensure that sufficient customer service staff is available to support cardholders.

Risk-based implementations, also known as Risk-Based Authentication (RBA), were designed to address historical concerns about the consumer experience when 3DS is implemented. RBA reduces friction at checkout, including the possible need for consumer enrollment, as it allows issuers to use a risk score to determine whether a particular transaction requires authentication.

Risk scores are derived by evaluating any transaction request presented to the issuer's access control server (ACS), based on variables such as transaction value, merchant type, location, and the device used to conduct the transaction. This evaluation is combined with the issuer's own knowledge of the cardholder's purchase history to estimate transaction risk. Issuers can use the risk score to determine the level of authentication they will require for each request, help focus their fraud prevention efforts on the most risky transactions, and thereby reduce friction for the consumer at checkout.

Use of RBA may require additional integration with the issuer's payment systems. Some solutions avoid the need for cardholder enrollment, even for risky transactions, by requiring cardholders answer a series of questions based on transactions recently made with the same account.

3DS vendors provide a variety of implementation solutions for issuers. Offerings range from standalone ACS products, which can integrate with an issuer's other supporting systems, to comprehensive on-behalf-of services that can even be integrated with an issuer's online banking system.

4.1.4 Impact on Acquirers

Acquirers are less involved in 3DS transactions than issuers or merchants. Acquirers register merchants who wish to participate in 3DS, to ensure that their agreements conform to the rules imposed by the different payment networks. Acquirers have to be able to accept the additional authentication data from participating merchants and process the data according to the participating payment system's requirements. The data must be accepted as part of the normal payment authorization, settlement, and clearing processes.

5 Securing Payment Data Using Tokenization

Tokenization secures payment data by replacing a primary account number (PAN) with a surrogate value, both to protect cardholder data and to help minimize the impact of a data breach. Tokenization can be very effective in both card-present and CNP channels, including mail order and telephone environments. However, tokenization should only be considered as a *complementary* fraud-prevention technique. Most of today's tokenization techniques leave a customer's PAN in the clear at some point in the payment chain (for example, when a card number is entered in a browser on a consumer's device or when the number is in the merchant's system before being exchanged for a token).

Multiple strategies are available for using tokens, and there is a recognized need to streamline these approaches and standardize the definitions. This section simply provides a brief introduction to tokenization architecture; the examples are not meant to cover all possible scenarios.

5.1 Tokenization Approaches

A tokenization approach currently used in merchant systems is sometimes called "acquirer tokens" or "non-payment tokens." As shown in Figure (labeled Acquiring Token - CNP), after the merchant sends the PAN to the acquirer, the acquirer returns a token in place of the card number. The acquirer stores the card number and related token in a secure token vault that can be accessed by the merchant whenever required. Implementing tokenization may reduce the number of systems that must comply with PCI Data Security Standard (DSS) requirements and therefore offers some PCI DSS relief. Since tokenized card data cannot be used to initiate payments, the stored card number data is not valuable to criminals. Tokenizing the card number, therefore, reduces the chance card data acquired inappropriately will be used fraudulently.

Other tokenization implementations involve replacement of an original payment credential (e.g., PAN) with an identifier (payment token), which may be used to complete payment and increase security. This approach reduces the risk of fraud from breaches both when used in new technology solutions and in existing payment systems.

Figure 6 shows several approaches for replacing a payment credential with a surrogate value or token. It assumes the cardholder arrives at the point of sale or the web site with their card and not the tokenized version of their card. There are models of tokenization where the consumer only presents a tokenized version of their card. This will not be the commonly accepted approach for the immediate future.

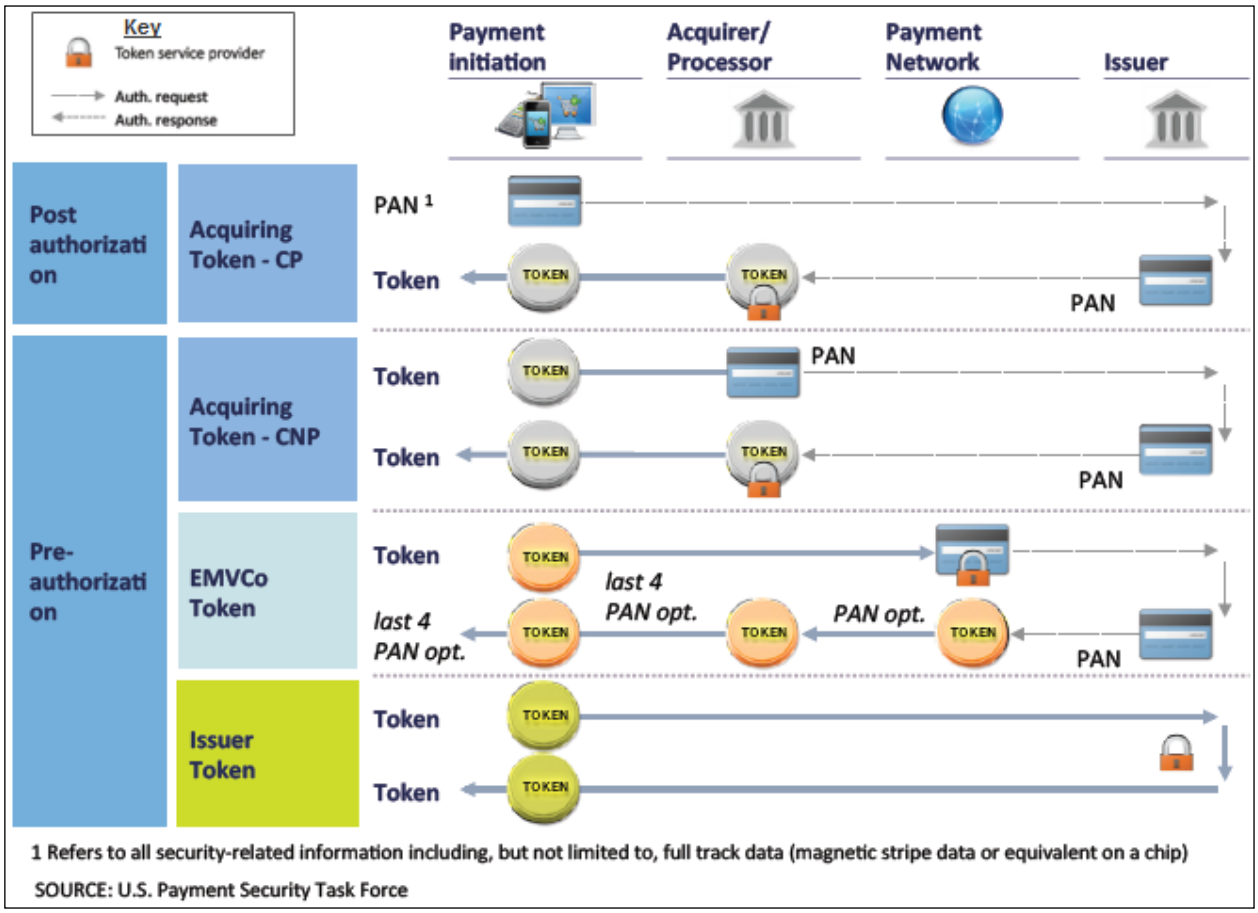
5.2 Impact on Consumers

In the prevailing model of tokenization, cardholders do not interact directly with tokens. However, they benefit from increased PAN security and lower fraud costs.

5.3 Impact on Merchants

Merchants can benefit from effective tokenization. When stolen card information propagates into the market, all merchants are potential victims. As tokenization becomes ubiquitous, it becomes more difficult for fraudsters to locate, steal, and use valid PANs or other payment credentials for fraudulent transactions.

Figure 6. Examples of Payment Tokenization Approaches[15]



Merchants may also enjoy a reduction in cyber-attacks and data breaches, as tokenized databases are less appealing targets. Stolen data is less valuable and over time tokenization may help to reduce attacks. Reduced exposure to clear-text PANs may also narrow PCI DSS compliance scope. A less tangible benefit is increased protection for merchants from damage to their reputations after a data breach. Customer trust can be difficult to rebuild after data theft.

Merchants may also experience lower customer service costs. When a customer's payment data are stolen, issuers typically reissue cards. When customers are on recurring payment plans, card reissuance may interrupt payments or present the customer with an opportunity to reevaluate and perhaps even stop a service. Even if the customer remains a customer, merchants may experience an increase in call volume as customers update their card information.

Adopting a tokenization scheme involves integration, regardless of whether the token is provided by a token service provider (TSP), a payment gateway, or an acquirer/processor. Merchants interested in implementing tokenization should consider currently available approaches as well as new alternatives and/or upgrade as they become available.

5.4 Impact on Issuers

Card issuers benefit from reduced fraud risk in the event of a data breach. Issuers also benefit by avoiding the inevitable consequences of a breach, including the expense involved in addressing customer inquiries,

[15] Provided by U.S. Payment Security Task Force as presented during the EMV Migration Forum in-person meeting in Chicago, September 2014. Note: "EMVCo token" is an alias for "payment token".

communicating with customers, and reissuing cards. In today's existing tokenization models, cardholders do not see or interact with tokens directly, except within cases of issuer tokens.

5.5 Impact on Acquirers

Acquirers benefit from a reduction in the threat of cyber-attacks and data breaches, as tokenized databases may be less appealing targets.

Unless the acquirer provides the tokenization service, merchant adoption of tokenization will have minimal impact on acquirers, assuming the token is structured to look like a PAN or similar payment credential. Acquirers will receive and use the token in place of the PAN as part of the transaction flow.

5.6 Other Considerations

Prior to implementing tokens, any stakeholder should consider how and whether their own processes and procedures may be affected, including but not limited to potential business implications relating to chargebacks, refunds, returns, reversals, and account updater services.

6 Conclusion

Although card-not-present fraud has been around in various forms for many years, CNP fraud attempts are expected to increase as EMV chip technology is adopted in card-present channels. And for merchants, CNP fraud can result in more than financial harm. In some cases, this type of fraud has a negative impact to brand reputation and can damage customer trust.

To reduce exposure to CNP fraud, merchants, acquirers, and financial institutions must work together to secure all of the sensitive data elements handled during transaction lifecycles. In protecting this data, all parties must be aware of potential effects on users, such as increased transaction times or tactics that make transaction completion more difficult. Several mechanisms can potentially reduce CNP fraud, reducing merchant financial liability and the overall cost of doing business.

No single security mechanism can protect against all possible fraud scenarios; rather, a systematic, layered approach must be implemented to secure all transaction data. These security layers must be able to protect sensitive data for the entire duration of the transaction. When properly implemented, such an approach will ensure that compromising a single data element does not affect the integrity of the other elements. Moreover, as set forth in Section 1, users may find a compelling business case for employing a "combination" approach, where implementing multiple security layers is likely to produce an integrated solution capable of protecting sensitive data.

The concepts and mechanisms discussed in this paper provide guidance regarding the different layers of security that can reduce the risk of CNP fraud. By introducing device authentication, merchants can greatly reduce their exposure to fraud before a transaction is presented for authorization. Exposure can be further reduced by implementing multi-factor authentication, which helps to ensure that the cardholders are authorized to carry out such transactions. Once a transaction is approved to be presented for authorization, tokenization can be performed to protect sensitive data both in transit and, eventually, at rest within the merchant environment. And, finally, fraud tools can be used at different points within the payment lifecycle to flag suspicious or risky transactions before final authorization.

In addition to cost considerations, implementation decisions will be influenced by an organization's specific risk policies and customer tolerance of disruption at checkout (which is likely to be different in different countries and cultures). If these are out of balance, it is unlikely the tools will deliver the desired results.

Although implementing these tools can be daunting, layers of security must be considered as the EMV chip card adoption cycle matures. Left unchecked, CNP fraud will materially impact vulnerable institutions and can affect the entire industry. Merchants, acquirers, and financial institutions are strongly encouraged to plan on phasing in these and other security practices as a high priority business requirement. Ideally, each stakeholder should address CNP fraud with their EMV chip migration strategy.

7 Publication Acknowledgements

This white paper was developed by the EMV Migration Forum Card-Not-Present Fraud Working Committee to provide an educational resource on the existing best practices for authentication methods and fraud tools to secure the card-not-present channel, given the potential increase in CNP fraud as EMV chip cards replace magnetic stripe only cards in the U.S.

Publication of this document by the EMV Migration Forum does not imply the endorsement of any of the member organizations of the Forum.

The project team who led the development of the white paper included: Co-chairs Sheryl York (Vantiv), Dennis Gamiello (MasterCard), and Joe Vasterling (Target) and co-leads Rodman Reef (Reef Karson Consulting) and Mike Strada (Chase Paymentech).

The EMV Migration Forum wishes to thank the Card-Not-Present Fraud Working Committee members for their contributions to the white paper. Special thanks go to Rodman Reef and Mike Strada for leading this project.

The following members participated in the development of the white paper:

The EMV Migration Forum would like to give a special thanks to X9 for their review of and feedback on the white paper.

- Philip Andreae, Oberthur Technologies
- Doug Black, Best Buy
- Kevin Bramlett, Union Bank
- Lori Breitzke, E&S Consulting LLC
- Ben Dominguez, Visa
- Francine Dubois, NagraID security
- Dennis Gamiello, MasterCard
- Pratap Gautam, American Express
- Randy Gibbons, Southwest
- Cliff Gray, Gray Consulting
- Neeraj Gupta, Vantiv
- Anne Hagen, Wells Fargo
- Jim Hays, CPI Card Group
- Deborah Herman, SunTrust
- Mary Hughes, Federal Reserve Bank of Minneapolis
- Elaine Jamer, Vantiv
- Alisha Johnson, Lowe's
- Deanna Karhuniemi, Chase Paymentech
- Keith Koval, UBS
- Amy Linden, MTA
- Cathy Medich, EMV Migration Forum
- Cheryl Mish, Discover
- Diana Molitor, FIS Global
- Todd Nuzum, Cubic
- Leslie Pollard, UBS
- Akif Qazi, Discover
- Eric Rainsberg, Macy's
- Rodman Reef, Reef Karson Consulting
- Henry Schwarz, Triton
- Megan Shamas, Montner & Associates
- Amrita Sinha, Lowe's
- Dan Smith, Wells Fargo
- Mike Strada, Chase Paymentecn
- Mike Strock, EMV Migration Forum
- Salman Syed, MasterCard
- Fernando Ulbrich, Morpho
- Shawn Usmani, NCR
- Jorge Vargas, Discover
- Joe Vasterling, Target
- Astrid Wang-Reboud, Gemalto
- Ainsley Ward, Clear2Pay
- Rebecca White, Barclaycard
- Sheryl York, Vantiv

Trademark Notice

8 Appendix A: Terms and Definitions

Term	Also Known As (AKA)	Definition
Access Control Server	ACS	3DS software incorporated into a card issuer's server that authenticates cardholders, approves transactions, and communicates over the Internet with other components of the 3DS ecosystem.
Authentication		Means by which a terminal/payment web site can validate a card as a valid payment device (i.e., not lost or stolen and not counterfeit) or verify that the cardholder is who he/she says he/she is. Authentication serves a vital function in protecting the identities of users.
Authentication Factors		Information used to identify a cardholder or other individual. There are three factor types: 1. The possession factor (something only the person can have); 2. The knowledge factor (something only the person knows); 3. The inherence factor (something only the person can be). Each authentication factor includes a range of data elements that can be used to authenticate or verify a person's identity. Security research has determined that for positive authentication for payments, at least two (and preferably all three) factors should be present and verified.
Authorization Hold	Card Authorization, Preauthorization, or "Preauth"	A common term within the banking industry used to describe the practice of authorizing electronic transactions initiated by a debit card or credit card. The balance is held as unavailable until the merchant clears the transaction or the hold "falls off."
Biometrics		Recognition methods relying on human characteristics and traits such as iris, retina, hand, voice, fingerprint, vein, and face. Biometrics are easy and quick, convenient and, in some cases, invisible to customers. As used in multi-factor authentication, biometrics support the inherence factor.
CVV/CVC/CID	Card Security Code	CVV – Card Verification Value, also known as Card Security Code, a security feature on payment cards. CVC – Card Verification Code, a security feature on payment cards. CID – Card Identification Number, a security feature on payment cards

Term	Also Known As (AKA)	Definition
Card-Not-Present	CNP	Payment card transaction where the cardholder does not present the card for merchant examination at the time of purchase, such as a mail-order transaction or a purchase made over the telephone or Internet. Card-not-present transactions are a major source of card fraud, because it is sometimes difficult for a merchant to verify that the legitimate cardholder is conducting a purchase.
Display Card		A payment or non-payment card that is issued with a display screen that electronically generates its own security code, such as OTP or Dynamic CVV/C (dCVV/C)
Dynamic Card Verification Value/Code	dCVV, dCVC, dCVx	dCVx provide an extra layer of security for CNP transactions against payment card number theft. It replaces the static three-digit security code printed at the back of the card, by a mini-screen that displays a time-based code, which is automatically refreshed.
Dynamic IP Address		IP address assigned by a Dynamic Host Configuration Protocol (DHCP) server. The server typically assigns a different IP address each time the device connects to the network.
Facial Recognition		Biometric method that requires a device to view an image or video of a person's face and compare it to an image or video in a reference database. The comparison examines the facial structure, shape, and proportions; the distance between the eyes, nose, mouth, and jaw; the upper outlines of the eye sockets; the sides of the mouth; the location of the nose and eyes; and the area surrounding the cheek bones.
Fingerprint Recognition		Biometric method that compares two fingerprints, using the three basic patterns of a fingerprint's ridges: arch, loop, and whorl.
Hardware Security Module	HSM	A physical computing device that safeguards and manages digital keys for authentication and provides cryptographic processing.
Internet Protocol Address	IP Address	Number assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification addressing. Its role has been characterized as follows: A name indicates what we seek. An address indicates where it is. A route indicates how to get there.

Term	Also Known As (AKA)	Definition
Mail Order/ Telephone Order Transaction	MOTO	Form of card-not-present transaction where the order is placed over the telephone, by mail, or by fax.
Merchant Plug In	MPI	System incorporated into a merchant's web site that communicates over the Internet with other components of the 3-D Secure online payments ecosystem, such as by querying whether authentication is available for a card, sending an authentication request, and receiving an authentication response.
Micro Secure Digital	Micro SD	Small plug-in device that is an extension of the SD specification to cover input-output functions.
Mobile Network Operator	MNO	Provider of wireless communications services that owns or controls all of the elements necessary to sell and deliver services to a user, including radio spectrum allocation, wireless network infrastructure, back haul infrastructure, billing, customer care, provisioning computer systems, and marketing and repair organizations.
Multi-Factor Authentication	MFA	Refer to the definitions for Authentication and Authentication Factors.
One Time Password	OTP	Password that is valid only once, for a single login or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords, the most important one being that, in contrast to static passwords, OTPs are not vulnerable to replay attacks.
Out of Band	Out of Band	When authentication is conducted via a different channel than the channel used by the original transaction
Primary Account Number	PAN	Number assigned by an issuer to a debit or a credit card.
Payment Card Industry Data Security Standard	PCI DSS	The PCI Data Security Standard (PCI DSS) provides an actionable framework for developing a payment card data security process – including prevention, detection and appropriate reaction to security incidents.
Phishing		Attempt to acquire sensitive information, such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication using (for example) malware, social engineering, e-mail spoofing, or instant messaging.

Term	Also Known As (AKA)	Definition
Point of Sale	POS	Device where a customer pays. While POS once referred specifically to the credit card terminal at the cash register, POS now includes mobile, wireless, and virtual terminals.
Randomized PIN Pad		A keypad used to enter a PIN at e-commerce and similar sites where the individual keys change location each time a digit is entered. The next location of each key is not predictable from its previous locations.
Replay Attack	Playback Attack	Form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. Typically, a valid data transmission is intercepted by a fraudster, who then replays that transmission to authenticate his/herself fraudulently.
Secure Element	SE	Secure memory and execution environment that resides in a smart device or any mobile device in which application code and application data can be stored and administered and in which execution of applications occurs. The secure element is implemented with highly secure crypto chips (a smart card chip). The secure element provides delimited memory for each application and other functions that can encrypt, decrypt, and sign a data packet.
Subscriber Identity Module Subscriber Identification Module	SIM Card	Smart card chip that resides in a smart device or any mobile device that securely stores the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers).
Static Password		Access codes that are unchanging and always the same. Such codes are relatively more vulnerable to attacks.
Static PIN		A numeric password shared between a user and a system. Used to authenticate the user to the system. Typically, the user is required to provide a non-confidential user token (i.e., user ID) and a confidential PIN to gain access.
Token		Generic term for a placeholder or surrogate. In the context of payment card transactions, token refers to a surrogate card number that is submitted in the payment stream in place of the real card number, usually to protect against loss of the real card number due to compromised terminals, data breaches, or other payment stream compromises.
Token Service Provider	TSP	Entity that provides tokens to the payment card process as a means to reduce risk in handling high value financial instruments by replacing them with surrogate equivalents.

Term	Also Known As (AKA)	Definition
Tokenization		Process by which a placeholder or surrogate (token) is substituted for a card identification number. Typically, tokenization is a service offered by a payment network, acquirer, token service provider or third party service provider.
Trusted Execution Environment	TEE	Secure area that resides in the main processor of a smart device (or any mobile device) and ensures that sensitive data are stored, processed, and protected in a trusted environment. The ability to offer safe execution of authorized security software, known as trusted applications, enables the TEE to provide end-to-end security by enforcing protection, confidentiality, integrity, and data access rights.
Trusted Service Manager	TSM	Service role in a Near Field Communication (NFC) ecosystem. The TSM acts as a neutral broker who sets up business agreements and technical connections with mobile network operators, phone manufacturers, or other entities controlling the secure element in mobile phones. The trusted service manager enables service providers to distribute and manage contactless applications remotely by allowing access to the secure element in NFC-enabled handsets.
Two-Factor Authentication	2FA	Authentication method that involves satisfying two of the three authentication factors (ownership, knowledge, and inherence).
3-D Secure	3DS	Messaging protocol that enables real-time cardholder authentication during an e-commerce transaction. Solutions using 3-D Secure provide e-commerce merchants with greater security for payment card transactions when the cardholder is not present.
Voice Recognition		Process used to identify who is speaking. Voice recognition can be used to authenticate or verify the identity of a speaker as part of a security process.

9 Appendix B: CNP Definition

9.1 Background

Past experiences in several markets have shown that fraud migrates away from the physical point-of-sale (POS) toward other channels – most notably card-not-present (CNP) – as EMV is introduced. The objective of this whitepaper is to educate EMV Migration Forum members and others about current best practices including the existing authentication methods and fraud tools designed to secure the CNP channel.

Weighing the audience's need for timely, practical, and relevant information, this white paper has intentionally and deliberately limited the definition of what constitutes a CNP transaction.

This appendix contains payment industry definitions of CNP, related industry terms and acronyms, as well as some high-level use cases. These are all provided as they informed the overall data gathering process used in this whitepaper.

9.2 Industry CNP Definitions

- A transaction where both of the following conditions are true: a) The cardholder is not present at the merchant location; and b) The card is not present at the merchant location.
- Credit card, debit card or prepaid card transaction (conducted usually over the Internet, on a telephone or via mail order) during which the cardholder is not physically present and therefore his or her card is not seen, dipped or swiped.
- Card-not-present (CNP) refers to a purchase a consumer makes without physically presenting his or her credit, debit or prepaid card at the time of purchase.
- A card-not-present transaction (CNP, MO/TO, Mail Order/Telephone Order, MOTOEC) is a payment card transaction made where the cardholder does not or cannot physically present the card for a merchant's visual examination and use at the time that an order is given and payment effected, such as for mail-order transactions by mail or fax, or over the telephone or Internet.
- A CNP transaction is one where the actual card (i.e., the plastic card that has been provided to the cardholder by the card issuer) is not physically presented to the merchant location, and is therefore not seen, swiped, or dipped when a customer makes a purchase. Such transactions are most often conducted over the Internet (eCommerce), by telephone order (TO or IVR), or by mail order (MO). In all these cases, the cardholder does not or cannot physically present the card for a merchant's visual examination and use at the time that an order is given and payment effected.

9.3 Use Cases / Examples

Purchase Scenario	Cardholder Present	Card/Card Credentials Present	Card Physically Swiped or Dipped?	Results
Attended POS	Yes	Yes	Yes	Card Present
Unattended POS	Yes	Yes	Yes	Card Present
Mail / Fax / Phone Order	Yes	No	No	Card Not Present
e-Commerce	Yes	No	No	Card Not Present
In App Purchases	Yes	Maybe[16]	No	Card Not Present
Reoccurring Billing	No	No	No	Card Not Present
Deferred Billing	No	No	No	Card Not Present
Installment Payments	No	No	No	Card Not Present
Mobile[17]	Yes	No	No	Card Not Present[18]
IoT (Internet of Things)	Maybe	Maybe	Maybe	?

9.4 Related Terminology and Acronyms

- Synonyms
  - Card absent - In certain markets, this term is used interchangeably with CNP.
  - Distance payments - In certain markets, this term is used interchangeably with CNP.
  - Remote payments - In certain markets, this term is used interchangeably with CNP.
- CNP Segments/Types
  - ECom / eCommerce - The fastest growing subset of the CNP sector, most commonly done via Internet browser at a merchant website using a PC, a tablet, or a mobile device.
  - IVR - Interactive Voice Recognition. Orders made over a telephone (MOTO), where the consumer interacts with an IVR system rather than a live operator.
  - Installment payments - Where a purchase is made and the cardholder and the merchant agree that the final transaction amount will be completed over multiple payments. While the card may be present at the time of the initial payment, the merchant may not have access to the physical card for the remaining installments.
  - Mobile - A transaction where a mobile phone or other mobile device is involved in the initiation and confirmation of the payment. The transaction may involve the use of a web browser, be conducted via a mobile application (in-app), and or the use of a mobile wallet. (Note: Contactless

[16] Are all of the required card credentials present? For example, if a card that is designated as chip and PIN card is used for an in-app purchase, is the PIN provided? Are there other card credentials which are also not available at the time of the transaction, e.g., the PAN?
[17] I.e., Where a mobile device's browser is used to initiate the payment transaction.
[18] There are solutions designed to work on a mobile platform that emulate regular magnetic stripe or contactless chip transactions that may be considered card-present. The specific implementation will define its designation. Merchants, issuers, acquirers, processors and others are encouraged to consult with their respective payment networks regarding all applicable rules, requirements, policies and procedures.

transactions at the POS using a mobile device are also referred to as "mobile;" those transactions, however, are considered card-present transactions[19].)

- MOTO - Mail Order Telephone Order - Where the customer submits an order to the merchant by speaking with a live telephone operator, interacting with an IVR system, or by transmitting order information via facsimile machine (fax).
- Recurring payments - Where the cardholder and the merchant agree to a transaction where multiple payments of some amount will paid on a regular basis over a period of time. While the card may be present at the time of the initial transaction, the merchant may not have access to the physical card for the remaining payments.

[19] Merchants, issuers, acquirers, processors and others are encouraged to consult with their respective payment networks regarding all applicable rules, requirements, policies and procedures.

10 Appendix C: 3D-Secure: Comparison of Versions 1.0.2 and 2.0

	Current	New Version
Version	1.0.2	2.0
Managing Organization	Visa Inc.	EMVCo[20]
Channels Supported	PC, with limited mobile	PC, with new features specifically designed for applications on smart devices (e.g., smart phones, tablets, wearables, set top boxes) and digital wallets
Applications Supported	Payment, expandable to non-payment uses	Allow for support of emerging application-based payment and non-payment uses
Messaging Format	HTTP, HTML, XML	HTTP, HTML, JSON
Issuer Controls	Supports standard and risk-based authentication models	Supports standard and risk-based authentication models, with the emphasis being on risk-based. Improved support for issuers to utilize their own out-of-band authentication methods.
Merchant Controls		Improved support for merchants to integrate the authentication process seamlessly into their checkout experiences, for both application- and browser-based implementations.
Other		Improved user experience by enabling intelligent risk-based decisioning though enhanced data elements that encourage frictionless consumer authentication. Simplified flows and performance enhancements Industry-leading security enhancements

[20] Additional information related to 3DS 2.0 development is available on the EMVCo website.