Payments Council
WHITE PAPER
Smart Card Alliance

Card-Not-Present Fraud: A Primer on Trends and Authentication Processes

A Smart Card Alliance Payments Council White Paper

Publication Date: February 2014

Publication Number: PC-14001

Smart Card Alliance
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

Table of Contents

1 Introduction

EMV adoption in the United States is proving to be a complex process that affects all stakeholders, requiring investment in new acceptance infrastructure, development of back-end processes to incorporate chip technology, and re-issuance of plastic card form factors, among other things. If history is any guide, however, the payments system after migration will substantially reduce fraud at the physical point-of-sale (POS).

Experience with EMV implementation in other countries indicates that one indirect consequence of EMV implementation is an increased incidence of fraud for virtual POS purchases, in what are often referred to as "card-not-present" (CNP) transactions. CNP transactions are just what the name implies: transactions in which the plastic card form factor is not presented to the merchant at the time of purchase (e.g., for purchases made on the Internet or by telephone). These are transactions that cannot be authenticated using "standard" processes used at the physical POS. CNP transactions require an alternative approach to cardholder authentication.

CNP transactions are not new. In fact, Internet and other types of e-commerce transactions are the fastest growing payments segment. But the combination of EMV adoption, which reduces opportunities for fraud at the physical POS, and growth in e-commerce is increasing transaction activity by both legitimate shoppers and fraudsters.

The industry has devised a variety of means by which to authenticate CNP transactions, and this white paper is a primer on the topic. The data and concepts described draw largely on the original work of others. The paper summarizes recent trends in e-commerce and various types of fraud. Both pre- and post-EMV implementation data from other countries is presented, substantiating the likelihood of increased CNP fraud after migration to EMV in the United States. The paper then briefly defines authentication and lists the building blocks commonly used to design authentication processes. The subject is considered from both the merchant's and the issuer's perspectives. The paper concludes with a brief discussion of historical approaches to combatting CNP fraud after losses have increased.

2 E-Commerce CNP Fraud

There is a general consensus that e-commerce has been growing at a healthy rate and is likely to do so for some time. Consumers are growing increasingly comfortable with shopping on the Internet as businesses continue to innovate. Based on the sales estimates shown in Table 1, over $200 billion of additional spending could flow through CNP transactions.

Table 1. U.S. Retail e-Commerce Sales Estimates by Year ($ billions)

	2012	2013	2014	2015	2016	2017
Forrester Research	231	262	291	319	345	370
JMP Securities	230	261	295	331	364	397
eMarketer	226	259	297	339	385	434
RBC Capital Markets	225	258	292	–	–	–
Cantor Fitzgerald	222	249	276	304	331	–
Robert W. Baird	–	247	272	299	329	–

Source: eMarketer, April 2013, Figure 154501

This growth will be a plus for the e-commerce merchant segment, but as e-commerce grows, exposure to CNP fraud will also continue to grow. As experience in other countries demonstrates, fraudsters consistently focus their efforts on e-commerce transactions once EMV is implemented at the physical POS.

2.1 CNP Fraud in Context

CNP fraud is only one category of fraud, and it currently does not account for the most losses. A 2010 report issued by Aite[1] summarized prevalent types of card fraud:

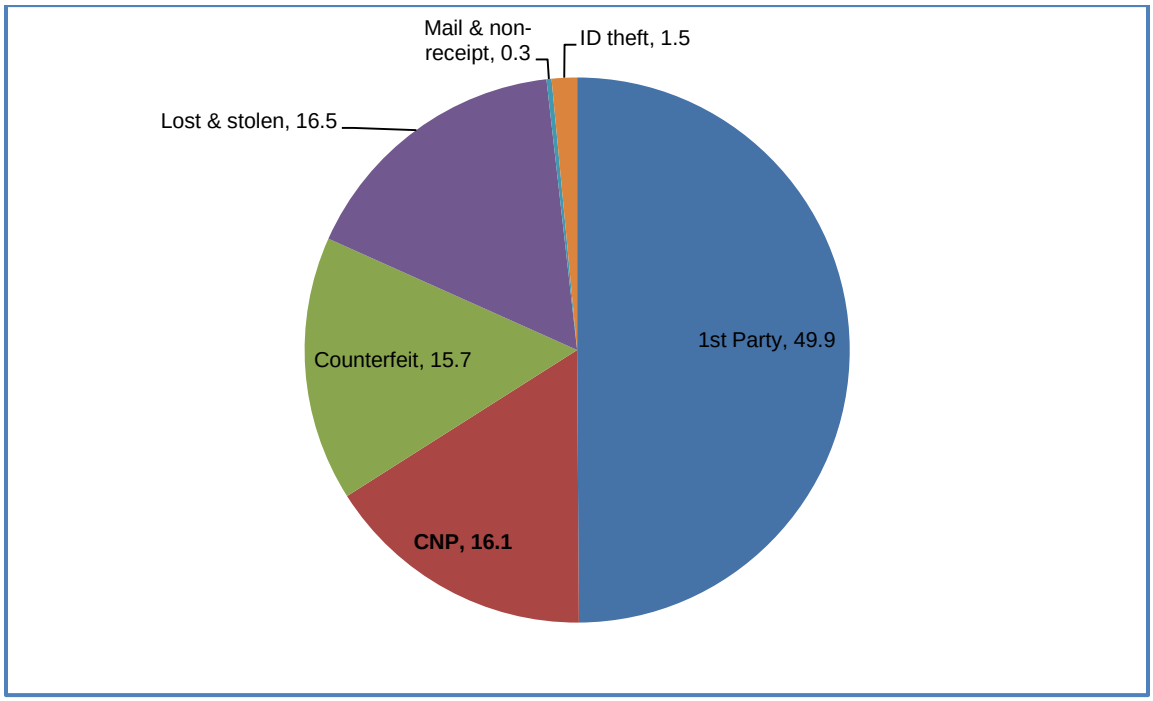
- **First-party fraud**, which occurs when a fraudster purports to be a legitimate cardholder or a legitimate cardholder intentionally decides not to pay off a credit card balance, leaving the card issuer with the debt.
- **CNP fraud**, which involves the unauthorized use of a credit or debit card number, the security code printed on the card (if required by the merchant), and the cardholder's address to purchase products or services in a setting in which the customer and the merchant are not interacting face-to-face, such as an e-commerce transaction or a transaction that takes place over the telephone.[2]
- **Counterfeit fraud**, which occurs when a fake card is created using compromised details obtained from the magnetic stripe or electronic chip in a legitimate card.
- **Lost and stolen card fraud**, which includes cards that are reported as lost or stolen by the original cardholder.
- **Mail and non-receipt fraud**, which involves intercepting legitimate cards while they are in transit from the issuer to the cardholder.

[1] Aite Group, *Card Fraud in the United States: The Case for Encryption,* January 2012
[2] Accertify white paper, http://www.accertify.com/documents/Accertify%20Whitepaper_CardNotPresentFraud.pdf.

- **ID theft**, which occurs when a fraudulently obtained card or card details are used to open or take over an account in the name of a legitimate user.

Source: Aite Group

Figure 1 shows down the fraud losses by category. As the figure shows, the Aite report attributes roughly 16 percent of total losses to fraud to CNP fraud.



Source: Aite Group

Figure 1. Fraud Losses by Category

According to a 2012 report recently released by Nilson,[3] card fraud losses in the United States totaled over $5.3 billion last year. Of that amount, an estimated 36 percent, or $1.92 billion, was borne by merchants. CNP fraud represented the largest category of losses for merchants. A Cybersource report found that e-commerce fraud is equal to 0.9 percent of e-commerce revenue, a higher proportion than for other forms of commerce.[4] In addition, a recently issued data by FICO shows that CNP fraud is growing faster than counterfeit fraud.[5] Statistics from different sources may vary, but there is clearly a large—and increasingly real—potential for losses due to CNP fraud.

[3] *The Nilson Report*, Issue 1023
[4] www.cybersource.com/US/Fraud-Report
[5] http://www.fico.com/en/Company/News/Pages/10-10-2013-FICO-Data-Shows-the-US-Credit-Card-Fraud-Incident-Rate-Rose-17-Percent-Over-Two-Years.aspx

2.2 Fraud Experience after EMV Adoption

Eighty countries globally are in various stages of EMV chip migration, including Canada and countries in Europe, Latin America and Asia. Table 2 summarizes EMV adoption by region as of Q4 2012.

Table 2. EMV Adoption Rates by Region (2012)[6]

Region	EMV Cards	Cardholder Adoption Rate (%)	EMV Terminals	EMV Terminal Adoption Rate (%)
Canada, Latin America, the Caribbean	401M	49.2%	5.6M	78.5%
Asia Pacific	372M	26.7%	5M	50.5%
Africa, the Middle East	50M	28.6%	0.6M	76.7%
Europe Zone 1[7]	755M	80.7%	11.7M	94.5%
Europe Zone 2[8]	46M	15.5%	0.9M	73.2%
United States	–	–	–	–
Total	1.62B	44.9%	23.8M	75.7%

Source: EMVCo. Data as of Q4 2012.

While it is impossible to present identical data for every country, available examples indicate that CNP fraud increases after EMV is adopted. EMV adoption in the UK and France (Europe Zone 1 region in Table 2), and Australia (Asia Pacific region in Table 2) all produced the same result (to different degrees): card-not-present fraud increased as a percentage of total fraud.

2.2.1 CNP Fraud: UK

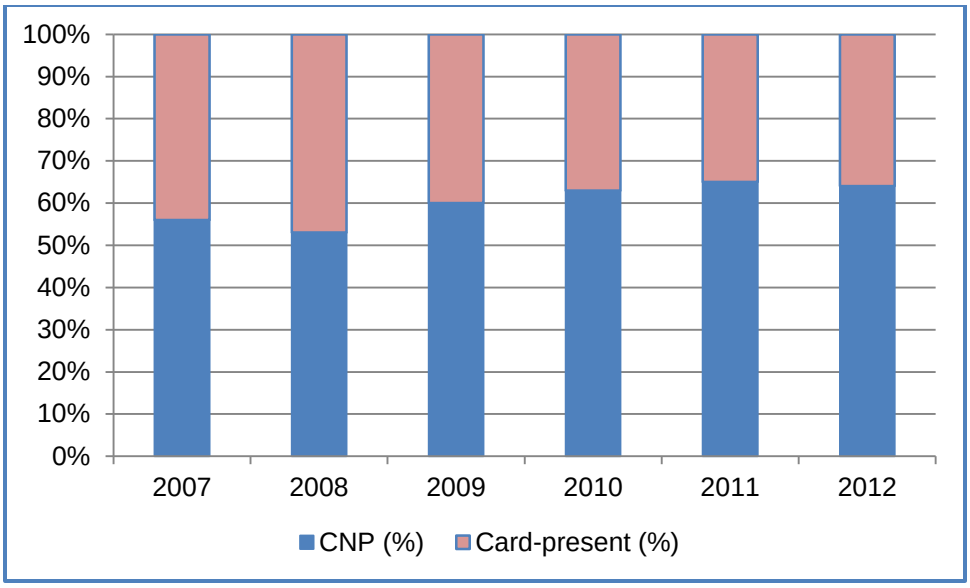
The UK Card Association has published CNP versus card-present fraud statistics covering the period from 2007–2012.[9] Fraud was reduced overall by £147 million, or roughly 27 percent, during this period. However, CNP fraud represents a larger percentage of total fraud (see Figure 2). While the UK adopted EMV in 2001, the liability shift did not occur until 2005.

[6] http://www.emvco.com/documents/EMVCo_EMV_Deployment_Stats.pdf

[7] Zone 1 countries include: Andorra, Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Gibraltar, Greece, Greenland, Hungary, Iceland, Ireland, Israel, Italy, Liechtenstein, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Caledonia, Norway, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, and UK.

[8] Zone 2 countries include: Albania, Armenia, Azerbaijan, Belarus, Bosnia & Herzegovina, Croatia, Georgia, Kazakhstan, Kyrgyzstan, Macedonia, Moldova, Serbia & Montenegro, Tajikistan, Turkmenistan, Russia, Ukraine, and Uzbekistan.

[9] http://www.theukcardsassociation.org.uk/plastic_fraud_figures/index.asp

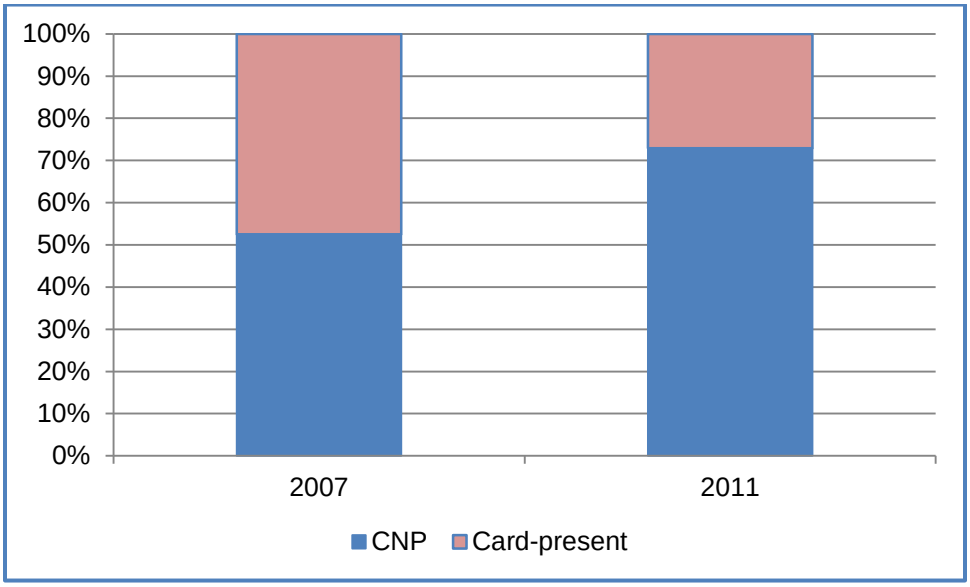


Source: UK Card Association

Figure 2. CNP Fraud Amount in the UK after EMV Adoption

2.2.2 CNP Fraud: France

The Observatory for Payment Card Security published similar data for France covering the years 2007–2011.[10] CNP fraud increased substantially (Figure 3).



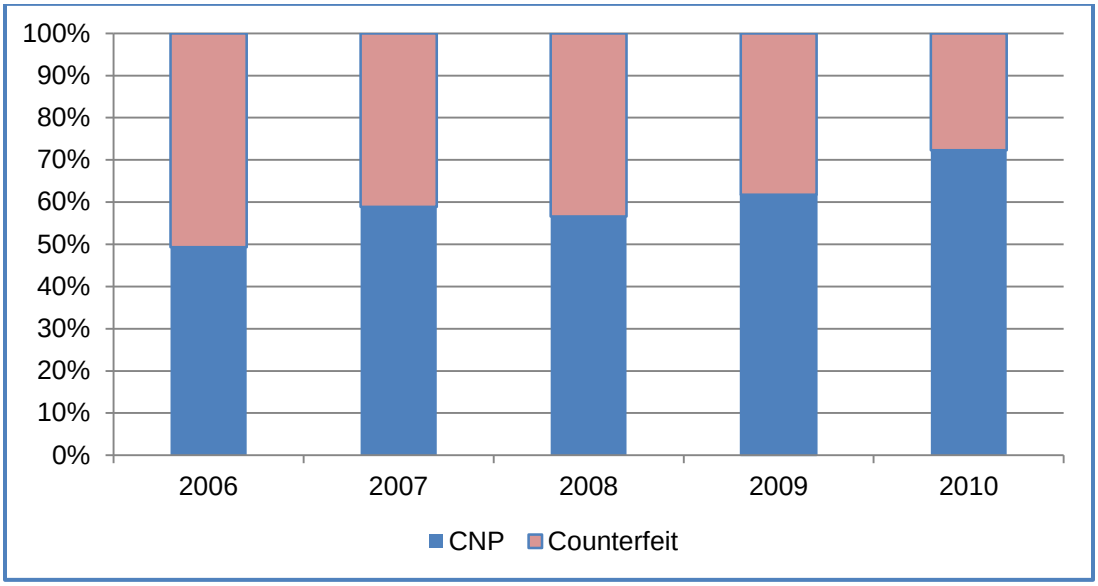
Source: Observatory for Payment Card Security

Figure 3. CNP Fraud Amount in France after EMV Adoption

[10] Annual Report of the Observatory for Payment Card Security, 2011

2.2.3 CNP Fraud: Australia

Data published by the Australian Payments Clearing Association confirm a similar experience in Australia. EMV migration occurred in 2008, and subsequent years saw a leveling-off and then a fall in counterfeit card fraud.[11] However, CNP fraud increased both in preceding and following years (Figure 4).



Source: Australia Payments Clearing Association.

Figure 4. CNP Fraud Amount in Australia after EMV Adoption

[11] Original: "Payments Monitor," Australia Payments Clearing Association, Second Quarter 2011, Secondary: "Chip-and-PIN: Success and Challenges in Reducing Fraud", Federal Reserve Bank of Atlanta, January 2012

3 Identity Authentication

An identity authentication process typically relies on a person providing one or more of the following, referred to as authentication factors:

1. Something the person has, such as a credit card, called an ownership factor.
2. Something the person knows, such as a PIN, called a knowledge factor.
3. Something the person is or does, such as a fingerprint, called an inherence factor.

Experts prefer to design authentication processes that require the presence of at least two (or ideally all three) factors (multi-factor authentication). Relying on a single factor implies extremely high confidence or tolerance for risk.

For the purposes of this discussion, identity authentication can be described as the process of ensuring that a transaction is being performed by the owner of the account that is being used for the transaction.

In a face-to-face transaction at the POS, a cardholder uses a plastic card (ownership factor) with a POS terminal reader, which transmits the necessary account information to the payment system. If prompted, the person enters a personal identification number (PIN, knowledge factor) or provides a signature, providing two-factor authentication. While CNP authentication methods are available, there are no commonly adopted authentication standards in use that are similar to the standards for authentication during face-to-face transactions; therefore, whatever the person knows deserves more scrutiny.

To mitigate CNP fraud, merchants, issuers, and cardholders must choose solutions that create an effective combination of the three factors from the available authentication building blocks.

3.1 Available Authentication Building Blocks

Authentication is achieved when the factor or factors provided by the cardholder match the factor or factors expected by the account issuer. The account issuer can be the issuer of the payment instrument (such as a credit card) or a merchant account that stores payment card information (such as an Amazon online account), among other things.

Table 3 summarizes currently available information used for CNP authentication.

Each CNP transaction type (Web, mobile, mail, telephone) includes information that can serve as an authentication factor and also offers a channel through which information the cardholder knows can be transmitted and verified. For example, Web site activity can provide the visitor's IP address (something the person has) and allow the person to input security information (something the person knows).

Table 3. Commercially Available Building Blocks for CNP Authentication

Channel	Available Ownership Factors	Available Knowledge Factors	Available Inherence Factors
PC or Web (e-mail)	Chip Single use account number IP address Tokens (static) Tokens (dynamic)	Personally identifiable information Passwords / PINs Security questions Account history Account information Tokens (dynamic) Address	__
Mobile or tablet (e-mail or SMS)	IMEI, MEID (device) IMSI, CSIM (subscriber) IP address Application Tokens (static) Tokens (dynamic)	Personally identifiable information Passwords / PINs Security questions Account history Account information Tokens (dynamic) Address	__
Mail	__	Address Post office box	__
Telephone (mobile or land)	Tokens (static) Tokens (dynamic)	Personally identifiable information Passwords Security questions Account history Account information Phone number Address	__

Merchants accepting CNP transactions often use commercial intermediaries to mitigate the risk of CNP fraud. Intermediaries typically standardize communication between the cardholder, merchant, and issuer or analyze relevant information to determine the appropriate level of scrutiny for a transaction.

The most obvious examples of standardizing intermediaries are the major card brands. Standardizing intermediaries can also include major e-commerce merchants who outsource their authentication solutions to smaller merchants (alternative intermediaries). These solutions first create or gather unique information and acceptable responses from cardholders. Programming interfaces then allow the information to be integrated into multiple merchant Web sites; during checkout, cardholders enter the information associated with their cards regardless of the particular merchant with whom they are interacting.

The second kind of intermediary performs a risk assessment of each transaction to allow for variation in the security approach. These assessments are made without the cardholder's knowledge, by referencing a variety of sources of information, such as other recent activity on the card, browsing history (cookies), or visitation history from that IP address. These approaches are referred to as "risk scoring" and "device fingerprinting."

Understanding these building blocks and generic categories is helpful for understanding different approaches to designing effective authentication methods. Table 4 summarizes a number of example authentication methods; it is by no means comprehensive.

Table 4. Example Authentication Methods

Authentication Method	Description
Static password or PIN	Shared secret known to both the customer and the merchant. Shared secret/PIN may be provided out-of-band, separate from the transaction itself.
Random static passwords	Typically a six-digit password that is created like other static passwords but not requested in its entirety on subsequent transactions. Instead, only 3 different digits of the password are requested for each purchase.
Static knowledge-based authentication	One or more secret questions asked to the user to confirm the user's identity.
Random knowledge-based authentication	One or more randomly selected secret questions asked to the user to confirm the user's identity.
End-point identity	Umbrella term that describes any of a number of methods used to identify the device by which the user is accessing the service provider.
One-time password using hard token	One-time password generated by a USB token, smart card, or mobile phone.
One-time password using soft token	Digital certificate.
Scratch card	Small card, often made of plastic, on which one or more areas contain information that can only be revealed by scratching off an opaque covering.
Bingo card	A numbered list of one-time passwords, printed on paper. For every e-commerce transaction, the user is required to enter a specific password from the list.
IVR voice verification	Consumer repeats a pre-recorded phrase or PIN to an IVR.
Chip Authentication Program (CAP) with personal card reader or mobile device	Dynamic password generated by an EMV chip card placed into a chip authentication reader and using a PIN.
Physical biometrics	An individual's biological characteristics.
Behavioral biometrics	An individual's physical behavior patterns.
Display card	A token in plastic card form with a display, an on-off button, and an optional PIN pad that generates a one-time password. The PIN pad allows the user to PIN-protect access to the one-time password and also sign transactions. If the card is an EMV chip card, it can act as both the chip authentication reader and the card.
Mobile device secure element	A chip embedded within a mobile device that stores payment account information and enables fully authenticated EMV transactions in the CNP environment. This could be used to support a number of the authentication methods in this table.

3.2 Merchant Perspective on CNP Authentication

For merchants, any of the CNP authentication approaches are technically feasible. The question is whether a particular approach is economically rational. Merchants must consider the following basic costs and advantages when evaluating CNP mitigation solutions:

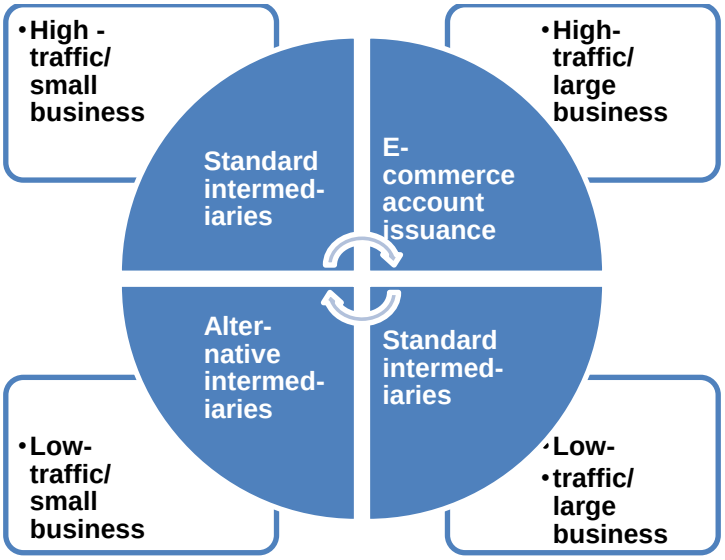
Hard Costs	Hard Advantages
• Required investment • Ongoing maintenance/compliance of systems	• Fraud reduction
Soft Costs	**Soft Advantages**
• Transaction abandonment • Consumer reluctance/fear of purchasing on the Internet	• Ease of purchase

Hard costs and advantages are relatively easy to determine: how much will the solution cost to build and maintain, and how much CNP fraud will it prevent. Soft costs and advantages are more difficult to estimate.

Generally speaking, the hard considerations are more important for smaller businesses with low-traffic customer bases; soft considerations are more important for large businesses with high-traffic customer bases. Smaller merchants are likely to rely more heavily on intermediaries for CNP authentication solutions. Larger merchants typically choose to assume responsibility for creating an e-commerce account that customers use to make purchases. Large merchants can design authentication processes that work best for their businesses since CNP fraud mitigation may not be the primary consideration. This dynamic is unlikely to change with the rollout of EMV in the United States; however, it is likely that the solutions will become more robust.

Currently, e-commerce merchants take three approaches to CNP authentication (shown in Figure 5): e-commerce account issuance, use of standard intermediaries, and use of alternative intermediaries.

Figure 5. Logical Authentication Facilitation by Business Type and Traffic Volume



3.2.1 E-Commerce Account Issuance

Large, high-traffic businesses typically choose to establish a unique e-commerce account for customers. There are many reasons for this, one of which is that it facilitates customer authentication. For example, one approach, which employs a variety of authentication methods, is as follows.

1. The customer initiates the account establishment process by providing a username, password, e-mail address, and telephone number.
2. To verify that the customer's information is valid, the merchant may send a dynamic token to the customer over e-mail or SMS, along with instructions for completing account establishment.
3. Once the customer uses the token to verify the information, security questions, shipping information, cardholder information, and billing information are gathered
4. The account is established.

In this example, to perform transactions, customers log on to their accounts using their usernames and passwords and make purchases using their stored information. If the merchant detects that a customer is accessing the Web site from a different IP address, the customer may be asked to enter responses to the previously established security questions. If a customer forgets a username, password, or the responses to the security questions, the e-mail address or telephone number provided previously may be used to repeat the tokenized process of re-activating the account.

It is also important to note that merchants must ensure that they comply with Payment Card Industry Data Security Standards (PCI DSS)[12] irrespective of how their system is configured or the level of outsourcing/intermediaries used.

3.2.2 Standard Intermediaries

Smaller businesses or businesses with lower-traffic customer bases often rely more heavily on intermediaries to facilitate cardholder authentication. In these instances, cardholder information is not stored but rather re-entered each time a purchase is made.

One fairly ubiquitous approach is to require the customer to enter information associated with the card that is not stored in the magnetic stripe, most commonly a static token (number) on the front or back of the card or the billing information associated with the card (in order to use the Address Verification Service (AVS)). Because this information can be verified at the back end but is not contained in the magnetic stripe, using it mitigates mass fraud, in the event that there is a massive breach of cardholder information. These approaches do not, however, prevent fraudulent activity when a card has been stolen. The information is equally available to someone in possession of a stolen card.

Another, less prevalent approach is very similar to e-commerce account issuance at the merchant level (described in the previous section): creation of an online account that is portable from merchant to merchant. The cardholder stores a username, password, security question responses, and similar information with the card issuer. The card brand provides the merchant with programming interfaces so that this information can be verified at the back end during checkout. This approach is less common because it is more difficult to coordinate—merchants must enable it, issuers must participate, and cardholders must sign up.

[12] See additional information on PCI DSS on the PCI Security Standards Council web site at: https://www.pcisecuritystandards.org/

Finally, card brands and payment gateways are developing a new approach in which transactions are assessed for fraud risk by analyzing a variety of proprietary data sources and using sophisticated fraud management techniques. Merchants can set strategies for authentication based on assessment scores.

3.2.3 Alternative Intermediaries

Alternative intermediaries provide small businesses with authentication capabilities identical to those enjoyed by large businesses that issue unique accounts. For example, PayPal is an alternative intermediary, providing an account that cardholders can use at a variety of merchants. Usernames, passwords, security questions, and additional information are stored by PayPal. Merchants are provided with appropriate programming interfaces, and the information is verified at the back end.

3.3 Issuer Perspective on CNP Authentication

If authentication is verifying that your customer *is* your customer, issuers must start seeing CNP transactions in those terms. Because merchants currently bear the costs of CNP fraud, issuers have done relatively little to combat it. For a variety of compelling businesses reasons, merchants—especially large ones—have made cardholders *their* customers, a byproduct of which is more control over fraud mitigation.

Standardized checkout procedures are valuable to cardholders. Remembering a multitude of usernames, passwords, PINs, and answers to security questions can be quite cumbersome. Card brands currently offer portable methods of authentication that work at a wide variety of merchants. Issuer participation is crucial if small and medium-sized merchants are to be convinced to incorporate these procedures into their checkout processes, but the processes must be designed to assuage merchant concerns over purchase abandonment.

Even though current CNP rules leave merchants liable for fraud, some issuers have long realized that combating CNP fraud would not only help restore consumer trust in e-commerce but could also avoid costly mass card reissuance if cardholder data are compromised. Issuers must consider the following basic costs and advantages when evaluating CNP mitigation solutions:

Hard Costs	Hard Advantages
• Required investment • Ongoing maintenance/compliance of systems • Cost of mass reissuance in case of suspicions of data breach	• Fraud reduction
Soft Costs	**Soft Advantages**
• Interchange loss because of transaction abandonment • Interchange loss because of consumer reluctance/fear of purchasing on the Internet	• Ease of purchase • Brand or relationship reinforcement

4 Payments Industry Responses to Increased CNP Fraud

While many different commercial solutions are used by e-commerce merchants to mitigate CNP fraud, the payments industry has implemented or announced three industry-wide approaches:

- Chip Authentication Program (CAP)/Dynamic Passcode Authentication (DPA)
- 3D Secure
- Tokenization

4.1 CAP/DPA

In order to address concerns about secure authentication for e-commerce transactions, the industry, led by the global payment networks, launched an initiative to leverage EMV deployments for dual factor authentication. This initiative is known as Chip Authentication Program (CAP) for MasterCard and Dynamic Passcode Authentication (DPA) for Visa. It uses the microprocessor and payment applications to generate a readable cryptogram similar to the one created by an EMV chip card that can validate that the user has an authentic card and knows the correct PIN, providing two-factor authentication that could in theory be used for traditional CNP transactions. These programs were launched in Sweden and the UK, with limited success.

The implementation requires both hardware (a secure reader for the cardholder) and system integration (for merchants and issuers). The required back-end updates and system integration meant that the deployments had practically no impact on most merchants with established Internet or telephone-based e-commerce services, and implementations were limited to financial institution Web sites (for e-banking).

CAP/DPA is used primarily as a strong authentication mechanism, which means that the one-time password is used to log into the e-banking Web site, thereby facilitating incremental services that require this strong authentication.

CAP/DPA is used in conjunction with MasterCard SecureCode and Verified by VISA to provide stronger authentication for e-commerce sites, which helps reduce CNP fraud. CAP/DPA can be used in various form factors – the traditional reader, a display card, and potentially a smart phone, so it remains a viable alternative for strong authentication in the e-commerce space.

4.2 3D Secure

Another CNP fraud tool supported by the payments networks is 3D Secure (which is a standardized protocol). (In the UK, CNP fraud leveled off as the use of 3D Secure increased.) Based on issuer preference and level of risk of the transaction, 3D Secure may require that a cardholder enter a static or one-time password (known also to the issuer or issuer processor), or may proceed with no additional authentication. Generally, 3D Secure has been more successful than CAP/DPA because investment and integration costs are lower and its impact on purchase abandonment rates and fraud prevention has proven attractive to merchants.

4.3 Tokenization Standard

In October 2013, three major card brands introduced a proposed framework for a new global standard for tokenization to make e-commerce and mobile transactions more secure.[13] Using this approach, the traditional consumer account number would be replaced with a digital payment "token" for e-commerce and mobile transactions. This approach would add a token requestor and token provider to the traditional payments data flow. The token would be used in the transaction, with consumers no longer being required to enter actual account numbers.

[13] https://newsroom.mastercard.com/press-releases/mastercard-visa-and-american-express-propose-new-global-standard-to-make-online-and-mobile-shopping-simpler-and-safer/

5 Conclusion

The implementation of EMV in the United States presents a number of challenges. However, overcoming these challenges and completing a successful rollout will substantially reduce counterfeit card fraud at the POS. An indirect but predictable consequence, however, is that the incidence of fraudulent CNP transactions will probably increase. A number of countries that have adopted EMV have seen increases in CNP fraud. For the United States, the problem is potentially exacerbated by the increasing amount of e-commerce transactions, as opposed to traditional face-to-face commerce.

Mitigating this increase in CNP fraud requires devising and implementing solutions for authenticating customers in CNP scenarios. There are a variety of different solutions currently in the marketplace; most rely on the use of a common set of authentication building blocks to get the job done. To date, merchants have chosen which solution to implement because they have assumed the risk of losses due to fraud and abandoned purchases. The approach taken by merchants varies by merchant size and visitation profile.

Because issuers have not been liable for CNP fraud, it is understandable that their role in preventing it has been fairly limited. Issuers can choose to participate in emerging processes for standardizing CNP authentication across merchants. Doing so will provide consumers with a more trouble-free experience when shopping virtually.

Past efforts to combatting CNP fraud on an industry level have met with mixed results. Approaches that required relatively less investment and appeared not to affect purchase abandonment rates achieved greater adoption rates, especially as supporting technologies and implementations have improved. The increased adoption of risk-based approaches and implementations using dynamic tokens has served to increase the adoption of 3D Secure.

As EMV migration proceeds, it is critical for the U.S. payments industry to take proactive steps to assist with mitigating the potential increase in CNP fraud. Identifying best practices strategies for merchants, evaluating industry-wide approaches that deal with risk at the payments system level, and engaging issuers in the fraud mitigation process are critical. Important factors for success will be not only effectiveness in reducing CNP fraud, but also ease of merchant implementation and customer ease of use.

6 Publication Acknowledgements

This white paper was developed by the Smart Card Alliance Payments Council to educate payment industry stakeholders about the impact of and need to further address card-not-present fraud in conjunction with migration to EMV in the U.S.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Payments Council members for their contributions. Participants involved in the development of this white paper included: ABnote; Capgemini; CH2M HILL; Chase; CPI Card Group; First Data Corporation; Gemalto; Giesecke & Devrient; Heartland Payment Systems; INSIDE Secure; MasterCard; NXP Semiconductors; Oberthur Technologies; SHAZAM; TSYS; Vantiv; Visa Inc.

The Smart Card Alliance thanks **Ryan Barnes**, TSYS, for leading the project and the following Council members who wrote content and participated in the project team for this document:

- **Philip Andreae**, Oberthur Technologies
- **Ryan Barnes**, TSYS
- **Deborah Baxley**, Capgemini
- **Philippe Benitez**, Gemalto
- **Jose Correa**, NXP Semiconductors
- **Allen Friedman**, TSYS
- **Sarah Hartman**, TSYS
- **Cathy Medich**, Smart Card Alliance
- **Astrid Wang-Reboud**, Gemalto

Payments Council members who participated in the review of the white paper included:

- **Philip Andreae**, Oberthur Technologies
- **Steve Arebalo**, INSIDE Secure
- **Ryan Barnes**, TSYS
- **Deborah Baxley**, Capgemini
- **Philippe Benitez**, Gemalto
- **Jose Correa**, NXP Semiconductors
- **Ben Dominguez**, Visa Inc.
- **Terry Dooley**, SHAZAM
- **Allen Friedman**, TSYS
- **Benoit Guez**, CPI Card Group
- **Sarah Hartman**, TSYS
- **Ron Hempel**, Chase
- **Jack Jania**, Gemalto
- **Geoff Keast**, ABnote
- **James Lock**, Chase
- **Christine Lopez**, Vantiv
- **Oliver Manahan**, MasterCard
- **Cathy Medich**, Smart Card Alliance
- **Bill Norwood**, Heartland Payment Systems
- **Nick Pisarev**, G&D
- **Matthew Radcliffe**, CPI Card Group
- **Paul Simon**, Chase
- **Brian Stein**, CH2M Hill
- **Sree Swaminathan**, First Data
- **Astrid Wang-Reboud**, Gemalto

Trademark Notice

About the Smart Card Alliance Payments Council

The Smart Card Alliance Payments Council focuses on facilitating the adoption of chip-enabled payments and payment applications in the U.S. through education programs for consumers, merchants, issuers, acquirers/processors, government regulators, mobile telecommunications providers and payments service providers. The group is bringing together payments industry stakeholders, including payments industry leaders, merchants and suppliers, and is working on projects related to implementing EMV, contactless payments, NFC-enabled payments and applications, mobile payments, and chip-enabled e-

commerce. The Council's primary goal is to inform and educate the market about the value of chip-enabled payments in improving the security of the payments infrastructure and in enhancing the value of payments and payment-related applications for industry stakeholders. Council participation is open to any Smart Card Alliance member who wishes to contribute to the Council projects.

7 Glossary of Terms

Account history. A payment account's purchase transaction history.

Account information. Important information associated with a payment card account, such as the cardholder's address.

Application. Program on a mobile device.

Biometrics. The use of unique human characteristics, such as fingerprints, as a means of authentication.

CDMA. Code Division Multiple Access mobile standard.

Chip. The computer integrated circuit in a mobile phone, tablet PC or payment card that can be used for authentication.

CSIM. The CDMA subscriber identity module that makes mobile phones interchangeable and is a possible means of identifying a subscriber.

Dynamic token. A fixed length token in which the character composition changes periodically so that the token cannot be compromised. For example, token 1234 becomes 5678 or some other 4-digit combination.

IMEI (International Mobile station Equipment Identity). A 15-digit number assigned to a mobile phone during production under international standards.

MEID (Mobile Equipment IDentifier). A 14-digit number assigned to a mobile phone during production under CDMA standards.

IMSI (International Mobile Subscriber Identity). A 15-digit number that is a possible means of identifying a subscriber under international standards.

IP address. Internet Protocol address (possible means of identifying a customer visiting an Internet merchant).

Magnetic stripe. A band of magnetic material to store data. Data is stored by modifying the magnetism of magnetic particles on the magnetic material on a card, which I then read by a magnetic stripe reader.

PII. Personally identifiable information.

PIN. Personal Identification Number.

Password. A secret word that only the customer and account issuer know.

Security question. Secret question and response that only the customer and account issuer know.

Static token. A token that is fixed in length and character composition.