Secure Payments: How Card Issuers and Merchants Can Stay Ahead of Fraudsters

Against a backdrop of growing vulnerability to fraud and breaches, merchants and card issuers must reinforce their secure payments infrastructure and processes, or risk losing customers to the competition. The best way forward is a layered approach in which commercial enterprises work with consumers to mitigate risk and improve fraud detection and prevention, our latest research reveals.
Executive Summary

Amid the continuing cat-and-mouse game of fraudsters probing payment infrastructures for vulnerabilities, as well as the passage of the EMV chip card migration deadline, the payments industry continues its struggle to plug security gaps. Criminals have upped their game and are attacking organizations on multiple fronts, and finding new ways to exploit loopholes in new technologies, even as organizations embrace them. This has increased organizations’ risk exposure, undermined consumer confidence in merchants and issuers, and threatened the integrity of the global payments industry.

To better understand the current state of payment security, we recently surveyed 509 U.S. consumers, 50 issuers and 52 merchants and acquirers. The survey findings were quite revealing:

- **Merchants have been slow to adopt technologies such as EMV, encryption and tokenization, even though these tools and techniques can enhance data security at various stages of the payment lifecycle.** On the issuer side, the EMV shift is taking longer than expected due to large installed bases and the associated card replacement costs. Fewer than 50% of issuers said they would replace magnetic-stripe cards completely by the end of 2015.

- **Merchants (66%) and issuers (78%) believe that as online shopping increases, fraud will shift to card-not-present (CNP) transactions** such as online and mobile commerce — regardless of EMV adoption — because criminals typically exploit new payments areas that offer the lowest resistance to fraud.

- **Card issuers and merchants admit to a lack of an in-depth understanding not only of the emerging vulnerabilities but also the solutions required to prevent new forms of fraud.** They also expressed low confidence in existing processes and solutions that can prevent fraud and data breaches. As a result, they plan to employ technologies such as artificial intelligence and advanced analytics, in addition to empowering consumers with tools to monitor and control their cards/accounts effectively.

- **On the flip side, consumers exhibit less confidence in the payment security provided by merchants than that of issuers.** They claim to be interested in taking charge of their card/account security and want to be better armed with tools to defend themselves against fraud.

- **Consumers also reaffirmed the conventional wisdom that they are reluctant to shop at stores affected by fraud or data breaches.** On the card issuer side, more than 80% of consumers are likely to shift to a competitor if their account security is compromised.

While merchants and issuers have put several security measures in place, a rapidly evolving payments landscape, combined with fraudsters’ increasing sophistication, warrants additional measures.
Overall, the survey clarifies the key concerns of merchants, issuers and customers and paints a composite picture of the array of initiatives underway to overcome security concerns (see Figure 1).

While merchants and issuers have put several security measures in place, a rapidly evolving payments landscape, combined with fraudsters’ increasing sophistication, warrants additional measures. We believe merchants and issuers should adopt a holistic approach that addresses all potential vulnerabilities and secures personal and transactional data throughout the payments lifecycle.

For merchants, this involves adopting a layered security approach, using a combination of EMV, tokenization and encryption to protect “card-present” transactions, as well as applying multi-factor authentication and internal fraud prevention tools to secure CNP transactions. Issuers should continue to strengthen their fraud monitoring and prevention systems and consider centralizing their anti-fraud efforts, in addition to providing customers with mobile tools and apps to control their account/card usage. Merchants and issuers should take it upon themselves to increase fraud awareness by continuously educating and communicating with customers.

Assessing Payment Security: A Customer, Issuer and Merchant View

Source: Cognizant Research Center
Figure 1
Digital Invades the Payments Landscape

A slew of technological innovations is sweeping the U.S. payments space, originating from financial technology (fintech) companies, established technology giants and mobile phone carriers, as well as merchants, social media businesses and non-banking players. All are seeking a share of the $354 billion North American retail payments market. Players such as Apple, Google, PayPal and Venmo are pushing the envelope by introducing innovative solutions that offer quicker and less expensive payments and money transfers (P2P payments). In fact, Wall Street banks are investing heavily in upstart fintech companies, which are expected to gain $4.7 trillion in annual revenues from traditional financial services companies, according to Goldman Sachs estimates.

Our study finds that merchants are beginning to support mobile payments (using technologies such as NFC, QR codes and beacons) for in-store payments. Apple Pay has established itself within a year of its launch (see Figure 2) as a go-to payments option. Nearly 60% of merchants said support of mobile payments was important or very important to their overall growth strategy. Currently, 44% of merchants support mobile payments, and 85% expect to do so by the end of 2016.

Moreover, more merchants are planning to add mobile point-of-sale (PoS) capabilities in their stores. M-commerce and e-commerce merchants are also beginning to support mobile payments.

Big banks, which had sat on the sidelines, are now gearing up to launch their own payment solutions (mobile wallets), in addition to supporting partners’ mobile wallets to provide customers with more choices. Our study reveals that about 54% of banks plan to offer mobile payment solutions (see Figure 3).
Digital currencies and cryptocurrencies are gaining acceptance as demand increases for faster and lower cost global money transfers. Despite their questionable origins, inherent flaws and controversies, digital currencies such as Bitcoin are being positioned as solutions to some of the payments industry’s long-standing problems, such as the extended processing times typically associated with checks and credit cards. Digital currencies allow users to transfer money, as little as a penny at a time, anywhere in the world within minutes. These transactions do not involve banks, and users are typically charged a nominal fee. Digital currencies can offer merchants a range of benefits over credit and debit cards. These include:

- **Lower transaction fees.** As there is no dependency on a trusted third-party, fees can be less than a dollar, compared with credit card fees of 2% to 5% and other charges.
- **Better transaction security.** The use of cryptographic algorithms makes digital currencies more secure. Further, users do not need to disclose any personally identifiable information.
- **Faster transaction settlement and relief from costly chargebacks and purchase returns.** This is possible because payments do not include credit card numbers or bank transactions.

Another looming threat – and opportunity – is the emergence of the Internet of Things (IoT), which will lead to many connected devices and even wearables being equipped with payment capabilities. (For more on this topic, read our white paper “Gearing up for the Internet of Payments.”) For instance, MasterCard has launched a program to turn a vast array of consumer products, such as wristbands, key fobs and jewelry, into payment devices. Visa is working on a connected car solution that allows consumers to pay for fuel, food, parking, etc. from their vehicles. Microchip implantation in humans is already a reality, with individuals and employees (e.g., Sweden-based Epicenter) using them to operate equipment such as phones, computers and photocopiers, as well as unlock doors and pay for food. The IoT’s endless possibilities are set to radically change the way payments are made in the future.

### Rising Threat of Fraud and Data Breaches

As merchants and issuers try to take advantage of the opportunities presented by the shifting payments landscape, they should be mindful of the lurking risks. Fraudsters are becoming increasingly sophisticated and are attacking merchants and issuers on many fronts.

**Cost of Fraud and Data Breaches**

The U.S. accounts for about 48% ($7.9 billion) of the global gross card fraud loss, although it represents only 21% ($6.2 trillion) of total card purchases. This is primarily due to the card industry’s continued dependence on older magnetic-stripe technology. This makes extracting sensitive card data easier for thieves who can use it to make CNP purchases and create counterfeit cards for card-present transactions. The average cost of fraud for merchants increased by 94% during 2014 through 2015, undercutting 1.32% of revenues.

Criminals are also using malware to break into merchants’ networks and steal card and customer details stored in back-end databases. Recent high-profile data breaches involved the installation of malware at PoS terminals – most of which still run outdated operating systems such as Windows XP – or database systems to copy large volumes of card data and customer records. The average data breach cost to U.S. businesses increased by about 10% from $5.85 million in 2014 to $6.53 million in 2015. Data breaches often lead to fraud, as criminals use stolen card data for purchases, as is reported to be the case at Home Depot.
The impact of fraud and data breaches goes beyond hefty chargebacks, penalties, stolen customer data and goods, and other financial and operational costs. It causes irreparable damage to an organization’s reputation. Our study puts this in sharp relief.

- Merchants affected by fraud or a data breach often struggle to regain customer trust. Consumers are particularly reluctant to return to merchants when their own data has been stolen (see Figure 4). In the case of banks, most customers are likely to switch to the competition if their online account is compromised (see Figure 5).

### Customer Reaction to Retailers Affected by Fraud

<table>
<thead>
<tr>
<th>Response</th>
<th>Will never transact</th>
<th>Will transact but pay only in cash</th>
<th>Will transact only if the retailer improves security</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>11%</td>
<td>28%</td>
<td>28%</td>
</tr>
<tr>
<td>Likely</td>
<td>16%</td>
<td>28%</td>
<td>18%</td>
</tr>
<tr>
<td>Do not know</td>
<td>6%</td>
<td>6%</td>
<td>6%</td>
</tr>
</tbody>
</table>

### Customer Reaction to Retailers from which their Data Has Been Stolen

<table>
<thead>
<tr>
<th>Response</th>
<th>Will transact only when there is no alternative</th>
<th>Do not know</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>20%</td>
<td>13%</td>
</tr>
<tr>
<td>Likely</td>
<td>21%</td>
<td>18%</td>
</tr>
<tr>
<td>No</td>
<td>18%</td>
<td>28%</td>
</tr>
</tbody>
</table>

Note: Percentages do not add up to 100 due to rounding.

Response Base: 509
Source: Cognizant Research Center
Figure 4

### Chances of Switching Banks if Online Account Is Compromised

- Highly likely: 30%
- Likely: 58%
- No: 6%
- Do not know: 6%

Response Base: 509
Source: Cognizant Research Center
Figure 5

### CNP Fraud: Poised to Explode

As the U.S. slowly adopts EMV to block card-present fraud, history reveals that fraud will shift to other payment channels with weaker defenses. CNP transactions are the obvious target because they only require a card number and CVV (card verification value) to make payments. While counterfeit card fraud declined by more than half in the UK from 2005 to 2008 after transitioning to EMV, the region also witnessed a 79% spike in CNP fraud in that timeframe. Canada, France and Australia witnessed similar spikes.12
Thieves have increased cross-border fraud in the U.S., which involves using stolen card data to conduct fraudulent transactions in another country, either through counterfeit cards or online purchases. As more U.S. merchants embrace EMV technology, which offers protection against counterfeit cards, CNP transactions are expected to become a bigger target for fraud.

Moreover, as merchants support new payment approaches across physical and digital channels, they are exposed to greater fraud risk. For instance, mobile payments accounted for just 14% of overall m-commerce transactions in 2014, but contributed to 21% of total fraudulent transactions.\textsuperscript{13} Further, chargeback rates for CNP transactions are higher than card-present transactions, which increases fraud costs for e-commerce and m-commerce players.

Our study reveals that about 78% of issuers and 66% of merchants believe CNP fraud will grow regardless of EMV adoption as virtual transactions increase and criminals hunt for new opportunities. Further, the growth in cross-border e-commerce and new forms of payments are likely to increase CNP fraud.

**Fighting Fraud: Security Improvement Measures**

Recent instances of fraud and high-profile data breaches have served as a wakeup call for the payments industry, which has started taking serious measures to improve security. Along with accelerating the mandatory shift to EMV, the industry is focusing on encryption, tokenization and multi-factor authentication, along with a host of internal tools and controls to limit fraud and improve transactional security.

Our research found that merchants and issuers are taking varying approaches to securing payments and shoring up their infrastructure and process vulnerabilities.

**Merchants**

Many merchants are implementing technologies such as EMV, tokenization and encryption to combat card-present fraud but are unprepared to deal with rapidly evolving CNP fraud.

- **EMV:** The U.S. is the last major country to adopt EMV chip technology in its payment cards. EMV cards contain embedded chips that generate a one-time code required to approve a transaction when used at an EMV-enabled PoS terminal. This validates the integrity of the card and prevents fraud through counterfeit cards. Also, as of Oct. 1, 2015, merchants and issuers that have migrated to EMV are exempted from financial liability for any card-present fraud.
  - **Adoption:** Nearly 80% of acquirers are working with their merchants on EMV migration and are focused on high-risk segments, such as retail, gambling and hospitality. Educating merchants about the ramifications of liability shift and changes to chargeback processing is still a work in progress for many acquirers.

- **Encryption:** Point-to-point encryption involves scrambling payment data as soon as it enters the PoS terminal to minimize exposure to sensitive data. The data is then sent via a secured network for processing, where it is decrypted by the payment processor securely without intermediaries. This protects data from hackers or other outsiders as it moves between various entities in the payments network.
  - **Adoption:** Nearly half of the merchants we surveyed have fully implemented encryption (see Figure 6, next page).
Tokenization: Merchants store large amounts of card data in their back-end systems for reconciliation, chargebacks, customer service, loyalty schemes, etc., making these systems an attractive target for criminals. Even if merchants encrypt payment data, the key must be stored with the data, which exposes it to theft.

Tokenization - which involves replacing sensitive cardholder data, such as permanent account numbers (PAN), with randomly generated alphanumerical characters (tokens) - greatly reduces the burden of storing sensitive data in-house. The merchant sends PAN data to a token service provider (TSP), which returns a non-sensitive token and stores the PAN in a highly secured database called a token vault. Merchants can use this token in place of the actual card numbers, so that even if thieves managed to steal the tokens, they would only find random numbers that are worthless outside the payments environment.

Adoption: About 46% of merchants surveyed have either fully implemented or are in the process of implementing tokenization (see Figure 7).

On-premise solutions are the preferred deployment model for about half of merchants that have already implemented or are planning to implement tokenization (see Figure 8, next page). Terminal vendor solutions (36%) and product solutions implemented in-house (36%) are the preferred tokenization standards vs. acquirer or in-house developed solutions.
Securing E-commerce and M-commerce Transactions

The merchants we surveyed use various tools to prevent e-commerce and m-commerce fraud (see Figure 9, next page). Address verification services (AVS) and card verification are still the most widely used solutions even for m-commerce, despite the fact that m-commerce and e-commerce pose very different fraud risks.

Since CNP fraud is expected to increase, merchants and financial institutions must consider advanced and more reliable authentication solutions or multi-factor authentication, using tools such as device authentication and biometrics. However, these tools are not in wide use. For instance, biometrics has been adopted by only 5% of the e-commerce merchants we surveyed.

Issuers

Issuers are working to address card-present fraud by replacing magnetic-stripe cards with new EMV chip cards. They are also providing customers with mobile tools that enable better control over their card/account security.

- **EMV**: The annual cost of counterfeit card fraud in 2015 was $3.6 billion.\(^{14}\)
  In the case of card-present fraud, issuers bear a larger share of fraud losses than merchants, which reinforces the need to quickly replace magnetic-stripe cards with EMV chip cards.

  However, issuers are replacing magnetic-stripe cards at a glacial pace due to high costs and a large customer base. Approximately 70% of issuers have replaced less than 25% of magnetic-stripe credit and debit cards with EMV cards, according to our research (see Figure 10, page 11). Only 42% of issuers indicated they will replace magnetic-stripe cards completely by year-end-2015, while another 38% said they plan to do so by year-end-2016.

  Many issuers are using more than one criterion for replacing magnetic-stripe cards with EMV chip cards. Only 42% said they are proactively replacing existing cards before they expire (see Figure 11, page 11).

- **Tokenization**: Issuers have historically been wary of tokenization, as they believed the approach ceded too much control to card networks that also act as TSPs. They were also concerned about strong consumer brands (e.g., Apple, Google, etc.) coming between them and their customers in the emerging m-wallet space. However, the benefits of tokenization in reducing issuer and customer risk, as well as securing actual card data, appear to have mitigated issuer concerns.

  Our research finds that 64% of issuers are currently using tokenization. Visa/MC/Amex tokenization approach is the preferred solution, followed by product solutions implemented in-house (see Figure 12, page 12).

---

**Merchants’ Tokenization Deployment Model**

<table>
<thead>
<tr>
<th>Model</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-premise solution</td>
<td>48%</td>
</tr>
<tr>
<td>Sourced to a tokenization service provider</td>
<td>36%</td>
</tr>
<tr>
<td>Hybrid solution (combination of on-premise and sourcing)</td>
<td>18%</td>
</tr>
</tbody>
</table>

*Note: Percentages do not add up to 100 due to rounding.
Response Base: 33 (includes only those respondents (46%) that have already implemented or are in the process of implementing tokenization)*

*Source: Cognizant Research Center*

*Figure 8*
Securing E-Commerce and M-Commerce Transactions

While EMV will reduce card-present fraud, issuers must brace themselves for an onslaught of CNP fraud. Our research reveals that issuers plan to implement the latest fraud prevention solutions (i.e., artificial intelligence to improve fraud detection) in the near future, along with traditional tools such as rules-based alerts and analytics to combat CNP fraud (see Figure 13, page 12).
Issuers are already using various customer authentication methods to prevent CNP fraud, with device authentication being the most used (see Figure 14, next page). Adoption of solutions that offer better protection of CNP fraud, such as 3-D Secure and biometrics, is still very low.

**Empowering Customers**

In addition to investing in security improvements, 46% of the issuers we surveyed are trying to empower customers with more control over their cards/accounts. Techniques include mobile tools and apps that allow customers to switch cards on and off remotely, and providing mobile alerts to customers when they detect suspicious activity (see Figure 15, page 13).

Among issuers offering such controls, 43% said a majority of their customers use them, and 48% report only partial adoption. Such tools can lead to improved loyalty, as noted by 75% of customer respondents, in addition to reducing the financial and security burden on banks.
**Issuers' Preferred Tokenization Solution**

<table>
<thead>
<tr>
<th>Solution Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visa/MC/Amex solution</td>
<td>56%</td>
</tr>
<tr>
<td>Product solution implemented in-house</td>
<td>38%</td>
</tr>
<tr>
<td>In-house developed solution</td>
<td>3%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
</tbody>
</table>

Response Base: 32 (includes only those issuers that have implemented tokenization)
Source: Cognizant Research Center
Figure 12

**Issuer Use of Fraud Prevention Tools**

<table>
<thead>
<tr>
<th>Tool Type</th>
<th>Currently Using</th>
<th>Plan to use in future</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction screening (software-driven)</td>
<td>48%</td>
<td>22%</td>
</tr>
<tr>
<td>Rule-based alerts</td>
<td>48%</td>
<td>22%</td>
</tr>
<tr>
<td>Analytics (predictive, pattern matching, etc.)</td>
<td>46%</td>
<td>20%</td>
</tr>
<tr>
<td>Transaction screening (manual)</td>
<td>44%</td>
<td>6%</td>
</tr>
<tr>
<td>Real-time fraud scoring</td>
<td>42%</td>
<td>22%</td>
</tr>
<tr>
<td>Neural networks</td>
<td>24%</td>
<td>24%</td>
</tr>
<tr>
<td>Artificial intelligence</td>
<td>14%</td>
<td>36%</td>
</tr>
<tr>
<td>None</td>
<td>6%</td>
<td>20%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Note: Percentages do not add up to 100 because multiple responses were allowed.
Response Base: 50
Source: Cognizant Research Center
Figure 13

**Customer Authentication Method(s) Supported by Issuers for Online and Mobile Transactions**

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device authentication</td>
<td>48%</td>
</tr>
<tr>
<td>Randomized PIN pad</td>
<td>34%</td>
</tr>
<tr>
<td>Multi-factor authentication</td>
<td>34%</td>
</tr>
<tr>
<td>Dynamic authentication (one-time password)</td>
<td>24%</td>
</tr>
<tr>
<td>Biometric solution (e.g., fingerprint, voice)</td>
<td>14%</td>
</tr>
<tr>
<td>3-D Secure</td>
<td>6%</td>
</tr>
</tbody>
</table>

Note: Percentages do not add up to 100 because multiple responses were allowed.
Response Base: 50
Source: Cognizant Research Center
Figure 14
When asked who should be accountable for fraud, 54% of consumers indicated that banks and merchants are equally responsible. However, 30% of customer believe merchants alone are responsible.

Confidence in Current Security Measures: A Reason to Worry

Merchants and issuers believe they are inadequately prepared to deal with growing security threats. Only 37% of merchants are very confident of their current fraud and data breach solutions (see Figure 16, next page). Issuers are more confident in card fraud prevention solutions than in CNP fraud solutions (see Figure 17, next page), but overall confidence is still low. Further, 60% of issuers do not know whether their organization takes an integrated or siloed approach to fraud prevention that incorporates different fraud prevention solutions for different payment channels.

When customers were asked how confident they were in the ability of issuers and merchants to protect sensitive data, 60% expressed high to very high confidence in issuers. When asked who should be accountable for fraud protection, about half (54%) of consumers placed equal responsibility on banks and merchants, while a third believe merchants alone are responsible (see Figure 18, next page). Interestingly, more customers are concerned about security when shopping on their mobile device than online and in physical stores (see Figure 19, page 15).

Consumers affected by fraud indicated that issuers were more quick to respond than merchants (see Figure 20, page 15); in fact, nearly one-third said merchants did not respond at all. In addition to communicating with customers, issuers are also taking swift remedial measures, our survey finds. Following the recent Apple Pay fraud, 34% of issuers developed more stringent Apple Pay sign-up processes for customers adding cards; 46% said they are now working with mobile payment companies to improve security.

Key Areas of Vulnerability

Despite the adoption of EMV, tokenization and encryption to secure data across the transaction lifecycle (see Figure 21, page 15), data vulnerability still requires organizational attention (see Figure 22, page 16), whether because of technology limitations or improper implementation. For example, in 2011, criminals in Belgium rigged EMV chip cards to accept any PIN input, as well as talk to the card issuer to gain transaction authorization. Card data can still be stolen from non-EMV merchants, while lost or stolen EMV cards can be used to make purchases in physical stores, as many card issuers support customer signatures instead of a PIN.
However, merchants that have not yet implemented any of the above technologies must review all the channels and links that carry card data and secure them using a holistic approach.

**Merchant Confidence in Processes and Solutions Used to Prevent Fraud and Data Breach Solutions**

![Confidence Levels Graph]

*Note: Percentages do not add to 100 due to rounding.*
*Response Base: 52*
*Source: Cognizant Research Center*
*Figure 16*

**Issuer Confidence in Current Processes and Solutions Used to Prevent Fraud**

![Issuer Confidence Graph]

*Response Base: 50*
*Source: Cognizant Research Center*
*Figure 17*

**Customer Opinion on Who is More Accountable for Fraud**

![Customer Opinion Graph]

*Response Base: 509*
*Source: Cognizant Research Center*
*Figure 18*
Customer Confidence in Merchants' Ability to Protect Card and Personal Data Across Sales Channels

<table>
<thead>
<tr>
<th></th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile</td>
<td>26%</td>
<td>40%</td>
<td>34%</td>
</tr>
<tr>
<td>Website</td>
<td>43%</td>
<td>43%</td>
<td>14%</td>
</tr>
<tr>
<td>Physical store</td>
<td>50%</td>
<td>37%</td>
<td>13%</td>
</tr>
</tbody>
</table>

Response Base: 509
Source: Cognizant Research Center
Figure 19

Banks' and Merchants' Response to Customers Affected by Fraud

Card Issuer (bank)
- Very quick response: 81%
- Responded slowly: 8%
- Responded after being contacted: 2%
- Didn’t bother to respond: 9%

Merchant
- Very quick response: 22%
- Responded slowly: 29%
- Responded after being contacted: 21%
- Didn’t bother to respond: 28%

Response Base: 199 (includes only those respondents affected by fraud)
Source: Cognizant Research Center
Figure 20

At a Glance: The Secure Payments Value Chain

Source: Cognizant
Figure 21
A Holistic Approach to Addressing Payment Security Challenges

Because the types of vulnerability in the payments ecosystem are both complex and evolving, it is imperative that merchants and issuers consider a holistic approach to address the risks. We suggest the following:

- **Merchants should adopt a layered security approach to prevent fraud and ensure secure payment data.**
- **Issuers should continue to improve their fraud monitoring and detection measures by centralizing fraud prevention efforts, and deploying real-time and behavioral analytics.**
- **Merchants and issuers should increase fraud awareness among cardholders by educating, empowering and engaging with them continuously.**

**Merchant Strategy: A Layered Security Approach**

Because no single solution exists that offers complete protection, we believe merchants should fortify payment security with multiple lines of defense, culminating in a layered approach.

- **Securing card-present transactions.** A layered approach to securing card-present transactions involves using EMV, tokenization and encryption. Organizations
should take the plunge by complying with the technical and operational requirements of PCI DSS. Although it does not guarantee complete protection – as seen in recent data breaches at merchants that adhered to PCI DSS guidelines – PCI DSS ensures a basic level of security and can form the foundation of a layered approach.

The next level of defense – and the core component of this approach – is EMV adoption. When combined with PCI DSS, EMV can enhance the security of payments data that reaches merchants’ systems. However, data is exposed once it enters the merchant’s network. Encrypting data at the PoS using point-to-point encryption can secure data against hackers while it travels between the merchant and processor (data in transit). Topping these layers with a tokenization solution – with token vault management provided by a sourcing partner rather than handled in-house – reduces the burden of managing sensitive data, vastly mitigating the fallout from data breaches (data at rest).

- **Securing CNP transactions.** Because CNP fraud is more complex, criminals committing such fraud are considered to be more sophisticated. Using multi-factor authentication – a process of verifying the authenticity of customers using at least two inputs, such as card number, PIN and biometric factors – can mitigate CNP fraud to a large extent. Merchants should also consider device authentication to identify devices that customers normally use for shopping before sending the transaction for authorization.

A case in point is Amazon’s multi-factor authentication, which requires customers to enter a code sent to their mobile device or generated by a smartphone authenticator app once they sign in with their existing username and password. This means thieves stealing a customer username and password would still require access to the mobile phone to log in. Enabling multi-factor authentication is a simple, one-time process. Customers can ask Amazon to remember each device, which will stop prompts for the code when that device is used. For PCs, the device refers to a specific browser (Chrome, Firefox, etc.).

3-D Secure adds a strong protective layer, as it requires cardholders to enter a static password (stored with the issuer) or a one-time password (generated by the issuer) sent to their mobile phones before paying for purchases. This can reduce chargebacks for merchants and shifts the liability to the issuer when a transaction is disputed.

Merchants should note that adding multiple authentications can negatively impact customers’ ease of purchase, and force them to abandon the transaction or the merchant. Behavioral and real-time fraud analytics can help merchants better understand customer purchasing trends and patterns, and preempt fraud attempts effectively.

**Key Considerations**

Merchants should consider the cost and complexity of implementing the aforementioned technologies. For instance:

- A small merchant that is compliant with PCI DSS and that processes low-value purchases may face fewer chargebacks and counterfeit card issues and, therefore, should focus on encrypting data both in transit and at rest.
- A large e-tailer may invest primarily in tokenization and strong customer authentication for safer online transactions.
- Similarly, a large merchant facing counterfeit card threat should consider EMV and data encryption, as well as tokenization, if data is stored in-house.
Merchants should implement network segmentation to prevent hackers from moving horizontally within the network. Merchants with an in-house token vault should use strong authentication to limit physical and virtual access to the vault. To mitigate the threat of data theft after de-tokenization, merchants should configure firewalls to restrict IP traffic and limit the number of applications that make de-tokenization requests to the token vault.

**Issuer Strategy: Centralize Fraud Risk Efforts**

Issuers responding to our survey indicated the prevalence of siloed approaches to fraud risk management, which can lead to redundant efforts, difficulty sharing risk information across departments, and the inability to gain a complete picture of the risks they face.

When organizations integrate their disparate risk management efforts in a centralized unit, they can better apply the intelligence gained from one channel or product to other risk areas, enabling them to more effectively quell threats and realize operational and cost efficiencies. Doing so requires organizations to consolidate the large amounts of customer and transactional data residing within silos and identify customers uniquely across channels and interactions to provide a unified view. By combining organizational data with data from external sources such as social media, and leveraging advanced analytics, organizations can produce deep insights into customer behavior that can help them detect anomalies early in purchasing behavior. These insights can also be used to provide alerts to customers, such as location-based fraud warnings, and reduce false positives.

**Involve Customers**

In addition to bolstering security, training employees and building an incident response team, merchants and issuers should also incorporate customers into their overall risk management efforts. We recommend that customers’ risky behaviors be continually studied and dealt with by employing a combination of the three Es:

- **Educate**: Customers must be continuously educated on various forms of fraud, precautions that can protect mobile devices from rogue apps, malware, etc., and steps to take if they suspect fraud.

- **Empower**: Empowering customers with tools that give them greater control over their accounts and improve security can go a long way toward improving confidence and driving traffic across channels. Issuers can provide mobile apps that allow customers to limit card spending in certain geographies, cap transaction limits, abort transactions, block and unblock cards, etc., which can mitigate fraud significantly.

- **Engage**: Engaging customers through regular communication using relevant channels in post-incident management is critical to increasing customer confidence and ensuring customer loyalty.
Research Methodology

The survey was conducted online in the U.S. in July 2015, and included 509 customers, 50 issuers and 52 merchants and acquirers.

Consumers

Gender Profile of Respondents

<table>
<thead>
<tr>
<th>Male</th>
<th>Female</th>
</tr>
</thead>
<tbody>
<tr>
<td>49%</td>
<td>51%</td>
</tr>
</tbody>
</table>

Age Group of Respondents

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-24</td>
<td>15%</td>
</tr>
<tr>
<td>25-34</td>
<td>21%</td>
</tr>
<tr>
<td>35-44</td>
<td>21%</td>
</tr>
<tr>
<td>45-54</td>
<td>20%</td>
</tr>
<tr>
<td>55-70</td>
<td>19%</td>
</tr>
<tr>
<td>Above 70</td>
<td>4%</td>
</tr>
</tbody>
</table>

Employment Status of Respondents

<table>
<thead>
<tr>
<th>Employment Status</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full-time employee</td>
<td>50%</td>
</tr>
<tr>
<td>Part-time employee</td>
<td>7%</td>
</tr>
<tr>
<td>Self-employed</td>
<td>6%</td>
</tr>
<tr>
<td>Homemaker</td>
<td>13%</td>
</tr>
<tr>
<td>Retired</td>
<td>12%</td>
</tr>
<tr>
<td>Student</td>
<td>6%</td>
</tr>
<tr>
<td>Unemployed</td>
<td>6%</td>
</tr>
</tbody>
</table>

Annual Household Income of Respondents

<table>
<thead>
<tr>
<th>Income Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than $30,000</td>
<td>20%</td>
</tr>
<tr>
<td>$30,000 to $49,999</td>
<td>25%</td>
</tr>
<tr>
<td>$50,000 to $74,999</td>
<td>21%</td>
</tr>
<tr>
<td>$75,000 to $99,999</td>
<td>18%</td>
</tr>
<tr>
<td>$100,000 to $149,999</td>
<td>11%</td>
</tr>
<tr>
<td>$150,000+</td>
<td>5%</td>
</tr>
</tbody>
</table>

Issuers

Respondents' Level in Organization

<table>
<thead>
<tr>
<th>Level in Organization</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vice-president</td>
<td>22%</td>
</tr>
<tr>
<td>Analyst/investigator</td>
<td>20%</td>
</tr>
<tr>
<td>C-suite (CEO, CFO, CTO and COO)</td>
<td>18%</td>
</tr>
<tr>
<td>Director</td>
<td>18%</td>
</tr>
<tr>
<td>Senior manager</td>
<td>14%</td>
</tr>
<tr>
<td>Fraud specialist</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
</tr>
</tbody>
</table>
Respondent Roles

- Deal with internal controls and solutions to prevent payment fraud: 68%
- Monitor/analyze/track/report payment fraud: 26%
- Deal with investigating fraud: 6%

Respondents' Organizational Department

- IT: 42%
- Fraud and risk management: 26%
- Compliance and security: 22%
- Operations: 8%
- Other: 2%

Annual Revenue of Respondent Organizations

- $1 billion - $9.9 billion: 50%
- $10 billion - $24.9 billion: 32%
- $25 billion - $49.9 billion: 8%
- $50 billion and above: 10%

Merchants and Acquirers

Respondent Type

- Merchant only: 65%
- Both merchant and acquirer: 33%
- Acquirer only: 2%
E-Commerce and M-Commerce Experience of Respondent Organizations

<table>
<thead>
<tr>
<th></th>
<th>Less than 1 year</th>
<th>Between 1 and 2 years</th>
<th>Between 2 and 4 years</th>
<th>More than 4 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-commerce</td>
<td>10%</td>
<td>21%</td>
<td>64%</td>
<td>5%</td>
</tr>
<tr>
<td>M-commerce</td>
<td>7%</td>
<td>29%</td>
<td>43%</td>
<td>21%</td>
</tr>
</tbody>
</table>

Note: Out of 52 respondents, 38 are involved with e-commerce, and 14 are involved with both e-commerce and m-commerce.

Note: All company names, trade names, copyrights and products referenced in this white paper are the property of their respective owners. No company referenced in this white paper sponsored this white paper or the contents thereof.

References


Footnotes

1. EMV stands for the first initials of Europay, MasterCard and Visa, the three companies that created the standard.


About the Authors

Vaibhav Shirke is a chief architect with the cards and payments business within Cognizant’s Banking and Financial Services business unit. With over 20 years of experience and acting as a solution architect, he leverages strong domain knowledge to map industry standard solutions to changing market demands. Vaibhav leads the secure payments initiative within Cognizant and works very closely with leading financial institutions and merchants in helping them define a secure payments roadmap. He can be reached at Vaibhav.Shirke@cognizant.com.

Rajeshwer Chigullapalli is the General Manager of Cognizant Research Center and leads the unit’s fact-based thought leadership program. He has more than 20 years of experience in research and publishing and has published numerous whitepapers on topics across the banking and financial services industry and in other industry sectors. He can be reached at Rajeshwer.Chigullapalli@cognizant.com | linkedin.com/in/rajeshwer-chigullapalli-508a01a.

Vinaya Kumar Mylavarapu is a Senior Research Associate with Cognizant Research Center, where he produces fact-based thought leadership across industries and sectors. He has more than 10 years of experience in business and industry research. Vinaya can be reached at Vinayakumar.Mylavarapu@cognizant.com | linkedin.com/in/vinayakumarmylavarapu.

Kamini Rajendran is Manager of Strategic Growth Opportunities within Cognizant’s Banking and Financial Services’ Payments Practice, a division focused on emerging trends in payments and establishing capabilities/ecosystems to support partners. She has over 13 years of payments domain experience and leads the secure payments focus area across industry verticals. She can be reached at Kamini.Rajendran@cognizant.com.


16 The Payment Card Industry Data Security Standard (PCI DSS) is a global standard for organizations accepting cards to protect customers’ payment card data throughout the transaction.
About Cognizant Research Services
With over 100 analysts, Cognizant Research Center (CRC) offers a wide array of business, market and strategy research services across nearly every vertical industry. CRC specializes in research-as-a-service (RaaS), an end-to-end offering through which research is delivered via a range of models – from traditional full-time-equivalent-based, through “pay per use” services. Through RaaS, CRC primarily addresses the unevenly distributed research needs of marketing teams, on demand. Learn more by visiting www.cognizant.com/business-process-services/research-analytics.

About Cognizant Banking and Financial Services
Cognizant’s Banking and Financial Services business unit includes consumer lending, commercial finance, leasing, insurance, cards, payments, banking, investment banking, wealth management and transaction processing. It is the company’s largest industry segment, serving leading financial institutions in North America, Europe and Asia-Pacific, including six of the top 10 North American financial institutions and nine of the top 10 European banks. The practice leverages its deep domain and consulting expertise to provide solutions across the entire financial services spectrum, and enables our clients to manage business transformation challenges, drive revenue and cost optimization, create new capabilities, mitigate risks, comply with regulations, capitalize on new business opportunities, and drive efficiency, effectiveness, innovation and virtualization. For more, please visit http://www.cognizant.com/banking-financial-services.