Prioritize Tokenization To Secure The Payment Chain

by Andras Cser, Ed Ferrara, and John Kindervag, April 27, 2015

KEY TAKEAWAYS

Improving The Security Of Consumer Payment Systems Is Mandatory
Fifty-year-old magnetic stripe and 20-year-old chip-and-PIN technology are no longer sufficient to secure mobile payments in the hostile world of eCommerce. S&R pros who protect the payment chain (cardholders, merchants, acquirers, processors, and issuers) need new methods to defend mobile payments and customer data.

The EMV Chip-And-PIN System Moves Fraud To Card-Not-Present (CNP) Payments
EMV created the chip-and-PIN system to combat skimming, which uses counterfeit magnetic stripe cards. European EMV adoption made skimming much harder, so fraudsters shifted to CNP payments. And customers have resisted adopting 3D Secure for securing CNP payments because it's inconvenient and hard to use.

Mobile-Based Payments Will Compete Strongly With Plastic EMV Chips In The US
Why? Because widely adopted smartphones and mobile devices offer lower personalization and delivery costs to issuers, more payment attributes to use in more effective fraud management for acquirers and issuers, higher security for cardholders via cardholder-to-device authentication, and higher security via tokenization to merchants.
Prioritize Tokenization To Secure The Payment Chain
EMV Is Not A Panacea For Card Payment Vulnerabilities
by Andras Cser, Ed Ferrara, and John Kindervag
with Laura Koetzle, Thomas Husson, Benjamin Ensor, and Claire O’Malley

WHY READ THIS REPORT
Is the credit card as US consumers know it dead? With the recent massive credit card data breaches at retailers such as Target and Home Depot, the payment industry is ripe for change. In this report, we extrapolate from a variety of variables, including those large customer data breaches; the payment liability shift that will happen in October 2015; the level of security of mobile and Europay, MasterCard, Visa (EMV) contactless payments; and mobile device adoption in the US topping 72%, to help security and risk (S&R) professionals chart the future course of the US payments market. Forrester expects that more secure, encrypted, and tokenized transactions on digital wallets, mobile-device-based near-field communications (NFC) virtual cards, and EMV contactless payments will prove strong competitors to plastic EMV chip-and-signature and chip-and-PIN payments in the US. Thus, Forrester predicts that plastic EMV won't achieve broad adoption in the US until 2020.

Table Of Contents
2 Secure Payments Are Essential For Customer Growth And Retention
3 Tokenization Must Be A Cornerstone Of A Secure Payment Ecosystem
5 What Does Plastic EMV Chip-And-PIN Uptake In Europe Augur For The US?
6 Large US Plastic EMV Chip Adoption Will Not Happen Before 2020
9 Digital Wallets And Mobile Payments Will Clash With EMV Plastic

RECOMMENDATIONS
10 Demand Tokenization From All Payment Chain Participants
11 Supplemental Material

Notes & Resources
Forrester drew from a wealth of analyst experience, insight, and research through advisory and inquiry discussions with risk professionals and other thought leaders.

Related Research Documents
Define A Compelling Strategy To Secure And Protect Mobile Moments
The Future Of Mobile Security: Securing The Mobile Moment
Master The Mobile Security Landscape
SECURE PAYMENTS ARE ESSENTIAL FOR CUSTOMER GROWTH AND RETENTION

Forrester predicts that US mobile payments will be a $142 billion business by 2019 (see Figure 1). As customers adopt this new method of payment, customer confidence and trust will be essential. Personally identifiable information (PII), payment card data, and even data on customers’ buying habits represent significant business intelligence assets, and if your customers can’t trust you to handle that sensitive data responsibly, they’ll defect to competitors. Thus, security and risk professionals need to view security now as a critical component of customer retention and customer service. Customers expect constant improvements to the payment chain’s protection of personal and payment data. Current trends indicate:

- **Hacking current point of sale (POS) technology is far too easy.** Breaches at many popular businesses were headline news in 2014. They were embarrassing and costly — and the fines and lawsuits are far from over. Many of these went undetected for a significant time causing a serious loss of customer data and goodwill. For example, Target’s security operations personnel received alerts of the intrusions, but they failed to distinguish them from the noise. Out-of-date and low-security POS technology, often sporting unpatched and unsupported Windows XP as their operating systems, made it easy for hackers to steal credit card numbers.

- **Breach costs are skyrocketing while goodwill tanks.** Home Depot spent approximately $43 million per quarter on remediating the payment data breach. Target spent a whopping $148 million on remediating the impacts of its credit card breach and lost its CEO and CIO in the process. In hindsight, these expenses were completely preventable had the company taken warnings from security technology and consulting partner FireEye. Furthermore, if either firm had employed full encryption and/or tokenization for customer credit card data, the breaches would’ve been far less damaging.

- **A security breach directly affects a retailer’s top and bottom line.** A recent study found that 44% percent of survey respondents were victims of a data breach and that 60% of Millennials had had their data stolen. Trust for retail is low, with 45% of US shoppers saying they don't trust retailers to keep their information safe. According to the study, after a security breach, 12% of loyal shoppers stop shopping at that retailer, and 36% shop at the retailer less frequently. For those who continue to shop, 79% are more likely to use cash instead of credit cards, and shoppers who use cash statistically spend less money, hurting sales.

- **Nearly ubiquitous mobile devices offer greatly improved security.** Today’s payment infrastructure was designed 50 to 60 years ago for people who paid in person at stores with plastic magnetic stripe cards (debit and credit). Today’s payment systems need to adapt to today’s technology and improved authentication capabilities and avoid retrofitting for the requirements of an obsolete payment system. New forms of secure payments (such as the Starbucks Card) can offer not only better payment security but also a cool factor that provides competitive advantage.
Digital commerce is becoming dominant. Forrester expects online retail sales in the US to reach $297 billion in 2014, or approximately 9% of all sales in the US. We’re forecasting a strong compound annual growth rate (CAGR) of 11.1% between 2013 and 2018 for US eCommerce, yielding approximately $444 billion in online sales by 2018. Payment security for online and CNP transactions is quickly gaining importance.

Figure 1 Mobile Payment Revenue Growth In The US

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.

Tokenization must be a cornerstone of a secure payment ecosystem

While modern payment technologies have some inherent security flaws, they provide improved security controls (see Figure 2 and see Figure 3). Contrary to what many parties in the industry would have us believe, EMV is not the perfect solution for all our security problems. Here’s why:

- While EMV makes skimming nearly impossible . . . Cards with magnetic stripes are fairly easy to duplicate today: If your server in a restaurant takes your card out of your sight, he or she can make a full copy of your card information — and you won’t find out until you receive your next statement with $3,000 worth of unauthorized charges. EMV plastic cards use a chip to verify the authenticity of the card and to confirm the purchase, which makes creating counterfeit (skimmed) cards much more difficult than it is with magnetic stripe (magstripe)-based cards.

- . . . EMV by itself could not have prevented breaches like Target’s, . . . EMV without tokenization does not encrypt or protect the card numbers and expiration dates transmitted during card transactions. EMV is largely a bolt-on to existing card technologies to support a
chip on the card that prevents counterfeiting, but it does nothing to prevent counterfeiting of cards (i.e., you can still copy the data and produce a counterfeit magnetic stripe card that will work at any magstripe terminal) or fraudulent online use of cards in CNP transactions.\textsuperscript{15}

\textbf{\ldots and encryption and tokenization could have prevented those breaches, without EMV.}

Encryption entails the scrambling of the card number by the POS terminal before it is sent anywhere on the payment network. Here are the steps for tokenization: For the first transaction with a new customer, the POS terminal sends the encrypted card number to a central Payment Card Industry Data Security Standard (PCI-DSS)-compliant tokenization service provider repository (safe).\textsuperscript{16} Second, the tokenization service then creates an entry in its database that links the card number to the cardholder’s name, address, phone number, etc. Third, it performs the payment authorization process in a normal way on behalf of the merchant. Fourth, it returns a token (not the credit card number) back to the merchant as proof of the payment transaction. For subsequent payments, the merchant only sends a token (and not the credit card number) to the tokenization service and the process continues at the third step.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{payment-method-vulnerabilities.png}
\caption{Payment Method Vulnerabilities}
\end{figure}

\begin{tabular}{|c|c|c|c|}
\hline
\textbf{Magnetic stripe} & \textbf{EMV contact} & \textbf{EMV NFC contactless} & \textbf{Mobile device NFC contactless} \\
\hline
\begin{itemize}
\item Payment application (PA) coding errors
\item Point of interface (POI) keypad/PIN reader compromise (device tampering, device logging, COM port hacking)
\item OS memory scraping
\item OS file scanning (e.g., Microsoft Windows pagefile.sys)
\item Network sniffing and data interception
\item At any point in the payment chain if the personal account number (PAN) and associated authentication is left unprotected the information may be stolen.
\end{itemize}
& \begin{itemize}
\item These cards are susceptible to the same vulnerabilities as magnetic stripe cards with respect to the vulnerabilities presented by the POI/keypad, PA operating system, and PA network.
\item EMV cards deployed in the US will also carry a magnetic stripe for backwards compatibility, allowing for fraudsters to use card data for card-not-present (CNP) fraud.
\item EMV tokenization may be breached through poor implementation of encryption process in the PA.
\end{itemize}
& \begin{itemize}
\item The same vulnerabilities as EMV contact type cards
\item Radio interception (proximity scanning) – card data can be stolen using proximity scanning technology to “read” the card data.
\end{itemize}
& \begin{itemize}
\item Radio interception (proximity scanning) – card data can be stolen using proximity scanning technology to “read” the card data.
\end{itemize}
\hline
\end{tabular}

Source: Forrester Research, Inc. Unauthorized reproduction or distribution prohibited.
### Figure 3 Payment Method Security Features

<table>
<thead>
<tr>
<th>Magnetic stripe</th>
<th>EMV contact</th>
<th>EMV NFC contactless</th>
<th>Mobile device NFC contactless</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Magnetic stripe" /></td>
<td><img src="image" alt="EMV contact" /></td>
<td><img src="image" alt="EMV NFC contactless" /></td>
<td><img src="image" alt="Mobile device NFC contactless" /></td>
</tr>
</tbody>
</table>

- **None.** Security is dependent on the PA as well as the vigilance of the merchant employee to detect potential fraud and abuse.
- **All card information is stored as cleartext on the magnetic stripe.**

- **Payment data on the EMV chip is encrypted and “tokenized” so that a merchant (or fraudster) does not have access to account holder data.**
- **Cards in the US will still have a magnetic stripe containing cardholder data for backward compatibility.**
- **Customer data is still at risk if the PA is poorly designed.**
- **Liability rules shift placing the financial burden on retailers in October 2015 if they accept payment using magnetic stripe POI and not an EMV POI in the advent of a fraudulent transaction. This should incentivize retailers to only accept payment with EMV type cards.**

- **Similar features as EMV cards**
- **NFC technology allows the payment to be made by waving the card near a compatible reader.**
- **NFC connections have been intercepted. If information is sent as cleartext, then customer data is at risk.**

- **Similar features to the EMV/NFC payment card.**
- **Smartphones add additional security through the use of e-wallet technology. This adds convenience in that e-wallets can store multiple credit card accounts under encryption.**

**WHAT DOES PLASTIC EMV CHIP-AND-PIN UPTAKE IN EUROPE AUGUR FOR THE US?**

The US’ current magstripe-based credit card payments will not be able to meet the challenges of security and authentication: They’re too easy to clone and counterfeit, and they provide only signature authentication during payment. EMV chip-based (largely chip and PIN) cards have been the norm in Europe and in Asia for about a decade. The UK Cards Association in a report published in 2011 said that credit card fraud in the UK dropped by 63%. As fraud management experts know, however, combatting fraud is like cutting off the head of a hydra, and European EMV adoption demonstrates this neatly:
Skimming teams stole PINs from chip-and-PIN EMV cards. With EMV cards, magnetic stripe skimming becomes difficult if not impossible. As a result, skimming teams changed their focus. After the payment chain introduced EMV chip-and-PIN, they moved to copying data and PIN numbers from the chip to produce counterfeit magnetic stripe cards that fraudsters could use with terminals that accept both magnetic stripe and chip-and-PIN card payments.18

Skimming teams moved to the US and to eCommerce. Skimming teams moved their operations into the US and continued skimming debit cards at ATM machines. Fraud in global online CNP payments has also increased significantly as a result: Fraudsters don't physically steal or skim credit cards. Instead, they steal them in bulk and sell them in underground forums.19

But the European liability shift did force an upgrade of terminals and cards. The liability shift (i.e., that the party that does not support EMV chip-and-PIN is responsible for fraud if the other party supports it) has caused issuers to issue chip-and-PIN cards that force merchants to upgrade legacy magstripe-only infrastructure to chip-and-PIN- and contactless-capable terminals.20

LARGE US PLASTIC EMV CHIP ADOPTION WILL NOT HAPPEN BEFORE 2020

The liability shift (which was designed to incentivize merchants to move from magstripe to EMV) in the US is set for October 2015, with the exclusion of ATMs where the liability shift will happen in 2016 and automatic fuel dispensers, where the liability shift will happen in October 2017. Despite the looming deadlines, Forrester expects that EMV chip-and-PIN and chip-and-signature adoption in the US will be slow.21 There are three main reasons why: 1) these technologies don't solve fundamental security and fraud issues; 2) the US payment market is remarkably complex; and 3) costly terminal upgrades will slow adoption or move adoption straight to contactless capability.

1) EMV Does Not Solve Fundamental Payment Security And Fraud Management Issues

All parties in the payment chain — including cardholders, merchants, acquirers, processors, and issuers — must prioritize payment security. Here are the problems that security and risk and fraud management experts who protect the payment chain must grapple with:

EMV does not protect against wholesale breaches of large numbers of credit card numbers. It is the mass data breaches and related media exposure that cost a lot of money for a merchant, not the individual fraudulent transactions — and EMV does not protect against card numbers being stolen and used fraudulently. EMV’s Payment Tokenization Specification — Technical Framework was only launched in March 2014, and thus it has not yet been widely adopted.22
The EMV chip is 20 years old and was a retrofit to the (much older) magnetic stripe. EMV chips contain the same data as magnetic stripes, albeit in an encrypted form. Further, the EMV chip was designed as a bolt-on to the existing magstripe-based infrastructure for card-present (CP) payments without taking into account the requirements for CNP fraud management because CNP transactions represented a tiny slice of 1995’s volume of payments.

3D Secure implementations never enjoyed broad acceptance. 3D Secure implementations (verified by Visa, SecureCode/MasterCard, American Express SafeKey) require a relatively significant investment for the merchant to buy and install the merchant plug-in (MPI) into the eCommerce portal to secure CNP payments. 3D Secure involves a number of web browser redirects, it can produce cryptic and hard-to-diagnose error messages, and ultimately it inconveniences and slows customers down.

US fraud management is more advanced because US customers tolerate less friction. The US payment chain has always prioritized reducing friction so that customers can transact as easily as possible. Consequently, US banks have built out advanced and largely retroactive fraud management capabilities. In contrast, European banks employ more preventive measures, such as stronger security and mandatory two-factor authentication for online banking payments. This means that US banks may be less interested in upgrading to EMV as they already have fraud management capabilities in place and might prefer to preserve the ease-of-use of plastic card/magnetic stripe payments.

2) US Payment Market Complexity And Maturity Are Daunting

It is seemingly easy to jump to conclusions and say that US EMV adoption will follow European EMV adoption. But a variety of differences between the two markets make this the wrong conclusion:

The US market is larger, more mature, and more complex than other markets. With 7,500 issuers, processors, and subprocessors, the US is the oldest, largest, and most mature market for card payments. Thus, there are many legacy solutions (magstripe-capable terminals, obsolete but cemented-in fuel dispenser POS terminals), which are hard to replace and upgrade. Because of much larger volumes of card transactions, different contracts between banks and payment networks, and the issuers’ ability to push back harder or move to a competitive payment card network (like Visa, MasterCard, and American Express), the payment card networks cannot levy penalties on US issuers on every magnetic stripe transaction as easily as they can in Europe. Furthermore, unlike in Canada, where the government-backed organization Advanced Card Technologies promotes EMV awareness, there is no central EMV awareness promotion body for the US.
- **The US payments market is getting fragmented fast.** While magnetic stripe payments still represent the overwhelming majority of transactions, Apple Pay (with built-in tokenization) and the Merchant Customer Exchange (MCX) also offer secure payments. Furthermore, LevelUp and other QR-code-based payment systems also offer secure and lower-cost payment alternatives to EMV.

- **Banks and other issuers lag in EMV card issuance.** There are approximately 1.2 billion credit cards in the US today. The cost of issuing a magstripe-only card is about 15 cents, while issuing an EMV card costs between $2 and $4. Thus, the upgrade from magnetic stripe to EMV could cost issuers as much as $4.8 billion in the US. Obviously, the liability shift will help drive card upgrades to EMV, but this remains a bitter pill for issuers to swallow. While the EMV chip card alliance estimates that 120 million Americans have already received their EMV chip cards (most of them chip-and-signature), research firm Software Advice estimates that 88% of US customers never made a payment with EMV chip cards.

### 3) Costly POS Terminal Upgrades Will Give Merchants Contactless Capability Too

Forrester expects that merchant adoption will be the key factor in the adoption of any new payment method. At some point, you will have to upgrade your terminals anyway, and you will get both chip and contactless. Once you have contactless, you can allow contactless payments, obsoleting plastic EMV-chip-based payments. Consider the following factors:

- **Magstripe-on-magstripe keeps the status quo in liability for fraud losses.** Even after the liability shift happens, if neither the issuer nor the merchant has EMV (chip or contactless) capabilities, the liability for fraud losses is unchanged. In these cases if the merchant retrieved all the necessary pieces of information from the cardholder and followed all of the rules and regulations, the financial institution would bear the liability for the fraud. Thus, if everybody does nothing (neither the smaller issuers nor merchants upgrade to EMV), liability stays the way it is; this clearly suits the merchants or at least qualifies as “better the devil you know.” Smaller merchants with predominantly in-person payments may be willing to absorb very rare card-present fraud losses to avoid spending $250 to $600 per terminal on upgrades.

- **Merchants are reluctant to immediately foot the bill for costly terminal upgrades.** Home Depot and Target responded to their data breaches by upgrading magstripe-only terminals to EMV chip and contactless capable readers. Additionally, that $250 to $600 list price range we cited for EMV chip and contactless terminals does not include the upgrade cost of network infrastructure. Forrester estimates that there are 11 million to 13 million POS terminals in the US, with EMV’s penetration at the time of writing being less than 10%. So this amounts to a whopping USD $3-billion cost just to upgrade payment terminals. Hence American Express is supporting its small merchants with $100 to help fund terminal upgrades.
DIGITAL WALLETS AND MOBILE PAYMENTS WILL CLASH WITH EMV PLASTIC

Because of the above, Forrester does not expect either EMV plastic chip-and-PIN or EMV plastic EMV-chip-and-signature to achieve broad adoption quickly in the US. Instead, Forrester expects that EMV plastic contactless, EMV mobile-based contactless payments (virtual cards on the secure element of an NFC capable mobile device/phone), and digital wallets (Apple Pay, Google Wallet, etc.) will fiercely compete with EMV plastic chip-and-signature and EMV plastic chip-and-PIN in the US payment card market. Here's why:

■ **US smartphone penetration is high.** Close to 72% of mobile phones in the US are smartphones. This high adoption by itself presents a great marketing (upsell, cross-sell, etc.) and security improvement opportunity for all participants in the payment chain to move beyond EMV plastic. NFC adoption in smartphones is quickly gaining ground with Apple's iPhone 6, the Samsung Galaxy S5/Alpha, and most other flagship phones sporting NFC.

■ **The cost of personalization of mobile-device-based cards is lower than plastic.** Forrester expects that a true American Express, MasterCard, Visa credit or debit card from one of the networks will be personalized on the secure element in a trusted execution environment of the mobile phone. In this scenario, consumers can use this NFC-chip-based virtual payment card for contactless payments. This greatly reduces issuers' costs related to personalizing (manufacturing and embossing) and mailing cards to cardholders.

■ **Robust smartphone-based security and authentication will boost payment security.** One of the shortcomings of plastic card systems is that cardholder authentication at CNP and CP payment time is fairly weak (usually a four- to eight-digit legacy pin, which is easy to remember and thus easy to shoulder surf and even eavesdrop to discover), and payment terminals can ask to bypass them (payment terminals can choose to ignore the PIN). Mobile devices can use built-in fingerprint readers, cameras, and microphones for biometric authentication with both CP and CNP payments. Furthermore, GPS and cell-phone-tower-based geolocation can geofence the cardholder at payment time.

■ **Fraud management of mobile payment transactions becomes more reliable and accurate.** Because mobile-device-based payments generate many more transaction context attributes (IP address, geolocation, sensor data, etc.), fraud management solutions can and should use this data to make better real-time decisions about the use of a payment card. The mobile phone can run mobile applications (PayPal, for example) that can also greatly increase the ability of enterprise fraud management (EFM) solutions from suppliers like ACI, FICO, and SAS to manage CNP payment transaction fraud without friction. Lowering customer friction and false-positive rates are key requirements for EFM departments and vendors.
Large digital wallet ecosystems and EMV contactless force adoption of contactless terminals. Adoption of Apple Pay, Google Wallet, MCX, CurrentC, and PayPal digital wallets, even though they compete with one another, will force merchants to upgrade existing POS terminals to support contactless as well as magnetic stripes and chips. Once POS terminals support contactless cards and NFC on mobile devices, Forrester expects that many US customers will migrate directly from magnetic strip to contactless payments.

Tokenization is easy and built-in with mobile payments. Storage of payment card account numbers is the biggest issue in many breaches like those at Sony and Mandarin Oriental. EMVCo's (the consortium behind EMV) tokenization is in a nascent state with low adoption, while MCX CurrentC, Apple Pay, Google Wallet and other digital wallets build in tokenization so that credit card account numbers are not exchanged on the Internet. There is also no need for a merchant to store credit card numbers with these digital wallet systems, resulting in merchants eventually spending less money complying with PCI-DSS. But S&R professionals should note that merchants can optionally store customer PII and attach the token to it, with merchants still able to optimize their marketing (and build stores of sensitive data that S&R pros still have to protect).

Recommendations

Demand Tokenization From all Payment Chain Participants

Forrester expects that by 2025 in the US, mobile and EMV plastic contactless payments will have a larger share of payment transactions by volume than EMV chip-and-PIN and EMV chip-and-signature card payment transactions. S&R professionals will need to contribute to helping accelerate the adoption of contactless payments, and thus better protect your customers’ data and reduce your company’s potential for a large-scale data breach. To do so, Forrester recommends the following:

- **Merchant S&R pros, drive magnetic stripe+chip+contactless-capable POS terminal purchases.** Spending the $250 to $600 per terminal will hurt, but pushing the liability for fraud to issuers who lag with their adoption of EMV cards or mobile payments will be a big benefit in the event of a breach.

- **Issuer S&R pros, push for EMV chip+contactless cards if you’re not already issuing them.** This will protect you from having to absorb fraud costs when the merchant’s terminal already supports EMV chip or contactless. Furthermore, look for EFM solutions that use the expanded context attributes (geolocation, etc.) of payment transactions.

- **All S&R pros, demand tokenization support.** In today’s hostile environment, storing card account numbers (whether in cleartext or encrypted) is clearly irresponsible. Work with processors and acquirers that provide out-of-the-box support for tokenization to avoid further data breaches.
SUPPLEMENTAL MATERIAL

Survey Methodology
ForecastView is a syndicated subscription service delivering access to more than 40 forecasts annually across North America, Europe, Asia Pacific, and Latin America.

Our forecasts employ a unique methodology: By leveraging consumer demand-side data balanced with company supply-side metrics, we provide a highly detailed understanding of each market. Forrester’s ForecastView service provides reliable insight into the online, mobile, and emerging technology markets. It offers a framework for understanding market drivers and inhibitors and helps clients to plan and prioritize investment decisions. ForecastView provides detailed data and market metrics from our major forecast models over a five-year period for the markets of eCommerce, consumer technology, mobile, online content, financial services, and interactive marketing.

As part of the forecast modeling, Forrester develops comprehensive historical and base-year market size estimates based on a variety of sources, including public financial documents, executive interviews, Forrester’s proprietary primary consumer and executive research, and analysis of the Internet traffic database.

All of Forrester’s forecasts are designed by a dedicated team of forecasting analysts who build the models, conduct extensive industry research, and manage the process of formally building consensus among Forrester’s analysts. Forecast analysts have backgrounds in investment banking, management consulting, and market research, where they developed extensive experience with industry and company forecasting.

ENDNOTES

1 The adoption of mobile payments is an evolution — not a revolution — and the evolution is well underway. Although the landscape of mobile payment providers is in an ongoing state of flux, the ecosystem and mobile capabilities are maturing, and consumer and merchant adoption is accelerating. Over the next five years, US mobile payments will grow to $142 billion. See the “US Mobile Payments Forecast, 2014 To 2019” Forrester report.

2 Customer service — both good and bad — affects revenue. Social media and web reviews amplify this effect. Using these channels, customer service experiences tend to be widely shared with friends, colleagues, and from there the broader public. Research conducted in 2013 shows that 62% of B2B and 42% of B2C customers purchased more after a good customer experience. The same research also showed that 66% of B2B and 52% of B2C customers stopped buying after a bad customer experience. Source: “The impact of customer service on customer lifetime value,” Zendesk, April 2013 (https://www.zendesk.com/resources/customer-service-and-lifetime-customer-value/).
During December of 2013, hackers broke into Target's systems, exposing customers' card data, names, mailing addresses, phone numbers, and email addresses. In January 2014, the retailer announced that the breach potentially affected 110 million customers, or about one-third of the US population. Home Depot customers felt the hacker's sting in September. Bad actors used the same malware that affected Target. In another case, hackers stole nearly three million credit cards due to two separate security breaches at Michaels, the US arts and crafts store chain. P.F. Chang's, the nationwide Chinese food chain, also fell victim to hackers in 2014. Hackers exposed credit and debit card data, as well as cardholder names and the cards' expiration dates. The company could not definitively say how many records hackers stole. Hackers compromised LaCie's customer database. The breach went undetected for almost one year, putting anyone who shopped between March 27, 2013, and March 10, 2014, at risk. Also, in 2014, eBay's database of names, phone numbers, encrypted passwords, email addresses, physical addresses, and dates of birth was compromised in late February and early March. Source: “The credit card breaches of 2014,” CNET (http://www.cnet.com/pictures/the-credit-card-data-breaches-retailers/).

In between the headlines and after the social media frenzy has died down, there are long-term lessons we can glean that will help all S&R pros improve their enterprise's overall security posture, their specific breach response capabilities, and their understanding and appreciation for privacy law and changing consumer sentiment on privacy. For more information, see the “Lessons Learned From Global Customer Data Breaches And Privacy Incidents Of 2013-14” Forrester report.

Outdated POS terminals represent a major contributor to credit card theft, but there are several others. The payment chain is vulnerable across the entire payment process. All of these systems are vulnerable to attacks. The other top vulnerabilities include weak firewall defenses, non-segmented networks, insecure remote access, and, not surprisingly, unaware employees. Source: Mark Cline, “Security Weaknesses: The Franchisee's Achilles Heel?,” ControlScan, December 12, 2014 (https://www.smbsecurityguide.org/security-weaknesses-the-franchisees-achilles-heel/).

News about security breaches is now so ubiquitous that business executives (and even some chief information security officers [CISOs]) may largely ignore them — unless, like the 2013 Target breach, it sets a new record for scope, or the attack itself represents a new attack vector and method (e.g., Heartbleed). However, in between the headlines and after the social media frenzy has died down, there are long-term lessons we can glean that will help all S&R pros improve their enterprise's overall security posture, their specific breach response capabilities, and their understanding and appreciation for privacy law and changing consumer sentiment on privacy. See the “Lessons Learned From Global Customer Data Breaches And Privacy Incidents Of 2013-14” Forrester report.


8 Security and risk professionals need to renew their focus on customer issues. This is especially true in the payment card industry. For more detail, see the “CISOs Need To Add Customer Obsession To Their Job Description” Forrester report.

9 Source: Deborah Salmi, “Millenials Take Responsibility For Their Own Cybersecurity,” Avast Blog, October 1, 2014 (https://blog.avast.com/2014/10/01/millenials-take-responsibility-for-their-own-cybersecurity/).


13 Consumers are “preshopping” across more categories on digital devices, including phones and tablets, while the availability of more information at shoppers’ fingertips even when they are on the go is a significant driver of the growth in cross-channel shopping. In fact, cross-channel retail sales are now more than four times larger than online sales. For more information, see the “US Cross-Channel Retail Sales Forecast: 2014 To 2018” Forrester report.

14 For more information on how more consumers are “preshopping” and the corresponding growth in cross-channel retail sales, see the “US Cross-Channel Retail Sales Forecast: 2014 To 2018” Forrester report.

Source: Forrester Research Online Retail Forecast, 2013 To 2018 (US), Q4 2014 Update.


Tokenization service providers include payment processors and acquirers and security vendors such as CyberSource, FirstData, Gemalto/SafeNet, Vantiv, and others.


19 Forrester’s estimate for the price of a working credit card number, expiration date, and card code verification (CCV) is about $1/card number. Underground merchants often offer customer service and guarantees and replacement of stolen card numbers that do not work.


The liability shift is, as Visa put it: “The party that is the cause of a contact chip transaction not occurring will be financially liable for any resulting card present counterfeit fraud losses.” Source: Visa (http://usa.visa.com/merchants/grow-your-business/payment-technologies/credit-card-chip/resources.jsp).

Source: Verifone (http://www.verifone.com/solutions-services/emv/).

21 Chip-and-PIN cards have a secure chip that stores the encrypted card account number, expiration date, and in some cases the PIN code. When making a card present payment transaction at a POS terminal, the cardholder must input their PIN code to authenticate himself in order to get a payment authorization. Chip-and-signature cards contain do not have a PIN code associated with them and thus only make skimming but not CP fraudulent payment impossible.


23 Retroactive fraud management means that instead of improving security of payment transactions and enforcing more stringent authentication of cardholders, fraud solutions scan payment transactions to filter out potentially fraudulent ones.

24 Best Buy and Wal-Mart are backing the MCX retailer-owned group payment system, of which Target is a member.


32 However, Forrester expects that plastic payment cards will be around for long time because of their simplicity.

33 Customers, merchants, and financial institutions are all eager for more-secure payment methods that will lower the costs and end the headaches of these constant breaches. See the “Brief: Apple Pay Signals A Fundamental Shift In Secure Payments Technologies” Forrester report.

34 Personalization means the embossing of the account number, cardholder name, or expiration date on the card and storing the above information on the magstripe and on the chip.

35 For more information on biometrics, see the “Market Overview: Voice Biometrics” Forrester report.

36 This is useful because it adds additional context to the use of the card and can limit fraudulent use. If a device, according to its GPS geolocation, is not physically present at the geolocation of the POS terminal, it may be a sign of fraud.

Forrester Research (Nasdaq: FORR) is a global research and advisory firm serving professionals in 13 key roles across three distinct client segments. Our clients face progressively complex business and technology decisions every day. To help them understand, strategize, and act upon opportunities brought by change, Forrester provides proprietary research, consumer and business data, custom consulting, events and online communities, and peer-to-peer executive programs. We guide leaders in business technology, marketing and strategy, and the technology industry through independent fact-based insight, ensuring their business success today and tomorrow.

About Forrester

A global research and advisory firm, Forrester inspires leaders, informs better decisions, and helps the world’s top companies turn the complexity of change into business advantage. Our research-based insight and objective advice enable IT professionals to lead more successfully within IT and extend their impact beyond the traditional IT organization. Tailored to your individual role, our resources allow you to focus on important business issues — margin, speed, growth — first, technology second.

FOR MORE INFORMATION
To find out how Forrester Research can help you be successful every day, please contact the office nearest you, or visit us at www.forrester.com. For a complete list of worldwide locations, visit www.forrester.com/about.

CLIENT SUPPORT
For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Focuses On Security & Risk Professionals

To help your firm capitalize on new business opportunities safely, you must ensure proper governance oversight to manage risk while optimizing security processes and technologies for future flexibility. Forrester’s subject-matter expertise and deep understanding of your role will help you create forward-thinking strategies; weigh opportunity against risk; justify decisions; and optimize your individual, team, and corporate performance.