BI INTELLIGENCE

BII Payments BII E-Commerce

The Payments Security Report: New security protocols aim to close the massive hole in online and in-store credit-card security

John Heggestuen | March 16, 2015

BUSINESS INSIDER

The Payments Security Report: New security protocols aim to close the massive hole in online and in-store credit-card security

John Heggestuen | **March 16, 2015**

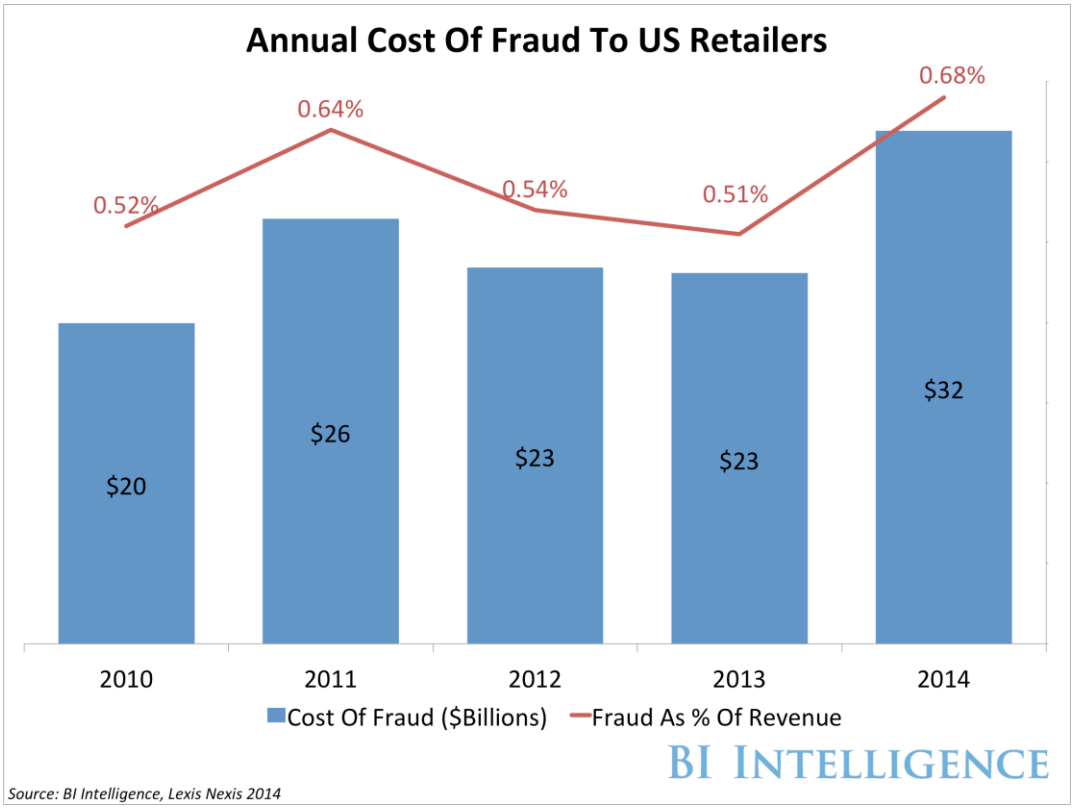
Key Points

- **The US has a huge problem with credit-card fraud.** In 2014, fraud cost US retailers $32 billion, about half of which was perpetrated using compromised payment-card accounts. To help solve this problem, card networks are pushing merchants to upgrade to EMV security, which is standard throughout other parts of the world.
- **EMV cards carry an embedded microchip for added security.** The microchip carries out real-time risk assessments on a person's card purchase activity based on the card user's profile. The chip also generates dynamic cryptograms when the card is inserted into a payment terminal. Because these cryptograms change with every purchase, it makes it difficult for fraudsters to make counterfeit cards that can be used for in-store transactions.
- **EMV will mitigate in-store fraud, but will also cause more fraud to move to online channels.** When fraud becomes more difficult to perpetrate in-stores, fraudsters will increase their focus on online merchants. Online transactions include a CVV number in addition

to the card number, expiration data, and other sensitive information. If this data is stolen it can be used to complete fraudulent transactions online.

- **To bolster security throughout the payments chain, encryption is becoming an increasingly popular security protocol.** Encryption degrades valuable data by using an algorithm to translate card numbers into new values.
- **Point-to-point encryption is the most tightly defined form of payments encryption.** In this scheme, sensitive payment data is encrypted from the point of capture at the payments terminal all the way through to the gateway or acquirer. This makes it much more difficult for fraudsters to harvest usable data from transactions in stores and online.
- **Tokenization increases the security of transactions made online and in stores.** Tokenization schemes assign a random value to payment data, making it effectively impossible for hackers to access the sensitive data from the token itself. Tokens are often "multiuse," meaning merchants can store them in their systems for subsequent transactions and not force consumers to re-enter their payment details. Apple Pay uses an emerging form of tokenization that allows consumers to make purchase across merchants with a single token.
- **3D Secure is an imperfect answer to user authentication online.** One difficulty in fighting online fraud is that it is hard to tell whether the person using card data is actually the cardholder. 3D Secure adds a level of user authentication by requiring the customer to enter a passcode or biometric data in addition to payment data to complete a transaction online. Merchants who implement 3D Secure risk higher shopping-cart abandonment.

Introduction



The US has an enormous problem with card fraud, and it is only getting bigger. Fraud cost US retailers, which see the bulk of their payments through card transactions, approximately $32 billion in 2014, according to our estimates based on data from Lexis Nexis and the US Census Bureau. That's up from $23 billion just one year earlier.

Fraud tends to target the weakest link in the card-processing system. That means consumers and merchants are targets for two reasons.

- First, there are more customers and merchants than there are payment companies and banks, so there are more opportunities to perpetrate fraud at these points in the payments chain.
- Second, while avoiding fraud is important, it's not as significant a concern to merchants and consumers as it is to payment companies.

> Because data security can make or break a payments company, the systems and databases for payments companies are typically well fortified against intrusion. (There are two significant exceptions in which payments processors were breached: Heartland Payments Systems suffered a breach in 2008, and Global Payments suffered a breach in 2012.) On the other hand, consumers' cards and card data and merchants' payments terminals, point-of-sales, and databases are typically much easier to access.

The fraud problem is why the US will over the next year upgrade to the EMV security standard. However, the EMV standard will primarily help mitigate in-store fraud, rather than card fraud overall. With in-store channels better secured, fraudsters will transition more of their activity to online and mobile channels. Late adopters of the EMV standard are also likely to see an increase in card fraud.

EMV stands for the names of the companies that created it — Europay, MasterCard, and Visa. For an in-depth look at EMV, read our report on the coming security upgrade.

In this report, we explore how the EMV migration in the US will shift the dynamics of fraud and the protocols that payment companies and merchants are implementing to protect their online and in-store channels. The explanations of each security protocol have been simplified for easier understanding.

In addition, in the table below, we provide an easy reference for the type of transactions each new security protocol is designed to protect, and a very basic description of how the protocol works.

5 Ways To Protect Card Transactions		
	Type Of Transaction Protected	**How It Works**
EMV	Offline	Authenticates card with dynamic cryptogram and user with PIN or signature.
Encryption	Online and offline	Degrades data by translating it into a new value with an algorithm.
Acquirer-Side Tokenization	Mainly online, some offline	Sensitive data is swapped for a new value with no logical relationship to original value.
Network-Side Tokenization	Online and offline	Sensitive data is swapped for a new value with no logical relationship to original value.
3D Secure	Online	User is authenticated by entering a password, biometric data or single-use passcode.

For the purposes of this report, here are the most important players in the card-payments chain to keep in mind:

- **Acquirers and processors** are synonymous for the purposes of this report. These are the companies that are responsible for processing payments, i.e., transmitting and securing payment data on behalf of merchants. They also often provide payment terminals for brick-and-mortar merchants to accept card payments.
- **Gateways** provide the technology for online merchants to accept card payments. They are the portal through which payment data flows before reaching a processor.
- **Issuers** are banks that issue credit cards to consumers.
- **Card networks** act as the hub within the card-processing ecosystem and serve two main functions: routing transactions between issuers and acquirers, and setting the rules by which the network of merchants, acquirers/processors, and issuers operates.

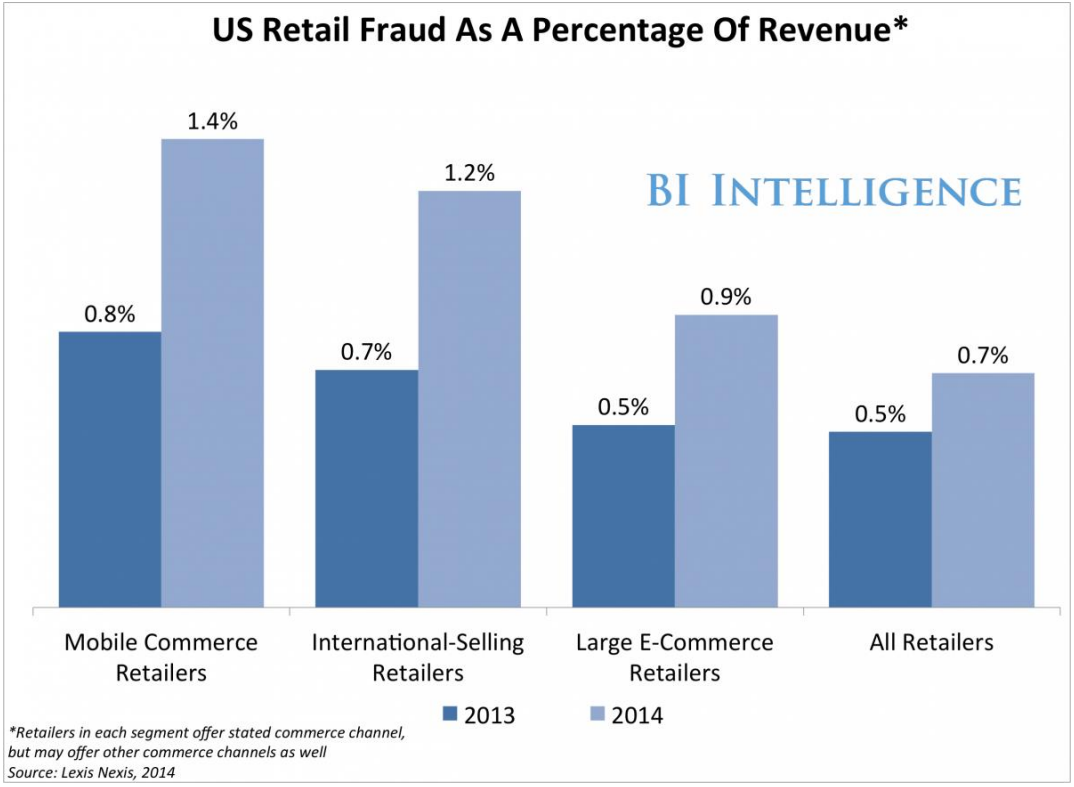
For background on how credit-card transactions are processed — please refer to our payments industry explainer.

Click here to download all the charts and associated data in Excel »

Click here to download a PowerPoint presentation of the charts »

The enormous fraud problem

US fraud costs reached $32 billion in 2014, a 38% increase over the $23 billion in 2013. This estimate involves fraud committed through unauthorized card transactions, fraudulent refunds, bounced checks, and lost or stolen merchandise. Over the past five years, between 30% and 50% of that fraud has been attributable to existing card fraud — meaning fraud perpetrated using information gleaned from consumers' existing plastic cards. This includes fraud perpetrated with counterfeit cards, card-not-present fraud (typically fraud committed via online and mobile channels), and lost-or-stolen card fraud.



Fraud already accounts for a larger share of revenue at merchants with online and mobile channels than it does in the retailer sector as a whole. And online and mobile's share of fraud will almost certainly rise once EMV is adopted.

This is simply because it is more difficult to tell who is using card data for a transaction made online.

- In most cases, retailers see a physical card before a transaction is completed in a store, something online merchants can't do. That means someone committing fraud in a store would need to have not only the card number, but also a counterfeit card. Conversely, a transaction made by someone using a stolen card number online cannot easily be identified as fraudulent by online merchants.
- In-store merchants also often check signatures or IDs to verify that those paying with a card are who they say they are when a transaction seems suspicious.
- By collecting signatures, in-store merchants are also less liable for fraud because they can produce evidence for their bank that they did their best to verify a person's identity. For these reasons, in-store merchants see a lower percentage of their revenue going to fraud (per the chart), given that they can sometimes shift the liability burden.
- In addition, committing in-person fraud doesn't scale as fast as online fraud. Online, fraudsters can buy and use many stolen card credentials without having to print out counterfeit cards to represent each individual account.

The heavier fraud burden placed on online merchants is clear in the data:

- In 2014, fraud costs were equivalent to 0.85% of revenue for large e-commerce merchants. These are merchants who may also have other commerce channels but maintain a strong online presence.
- For comparison, fraud costs were equivalent to 0.68% of revenue across all merchant segments.
- Merchants who offer mobile commerce platforms saw fraud reach 1.36% of revenue, higher than any other merchant segment. These merchants may take payments in store or online, in addition to via mobile.

It's important to note these fraud costs refer to how much merchants end up paying in chargebacks when fraudulent purchases are made at their store. This is different from the total fraud cost paid by Target Corp., for example, for the

massive data breach at its stores. Target may pay additional fraud costs beyond consumer chargebacks if proven liable for ineffective security.

For retailers and payments companies, mitigating fraud is about protecting themselves from both stages of fraud — from having card data stolen and thus incurring costs from liability, and from having fraudulent purchases made at stores, which most often must be paid back to consumers. Even if payments companies aren't necessarily responsible for bearing a heavy cost burden for fraud, their brands may be hurt by these incidents, which is why it's important to these companies to create better payments security systems.

Solving the fraud problem

Perhaps the best way to think about the future of fraud mitigation is to start with understanding how magnetic-stripe card fraud — the most common form of payments fraud — is perpetrated and how EMV is designed to mitigate mag stripe's vulnerabilities.

The magnetic stripe payment cards that are currently used in the US are relatively weak in terms of security. Payment data — including card numbers and expiration dates— is easy to skim off cards' magnetic stripes. This data can then be used to make counterfeit cards for in-store purchases. And if the fraudster happens to record the CVV on the back of the plastic card, the data can be used for online transactions as well.

To solve the in-store card-fraud problem, the major credit-card networks are pushing adoption of the EMV security standard.

EMV

Plastic EMV cards are similar to magnetic-stripe cards but with a key difference: EMV cards carry an embedded microchip. The microchip carries out real-time risk assessments using issuer-defined parameters. The chip also generates dynamic cryptograms when the card is inserted into a payment terminal.

EMV card

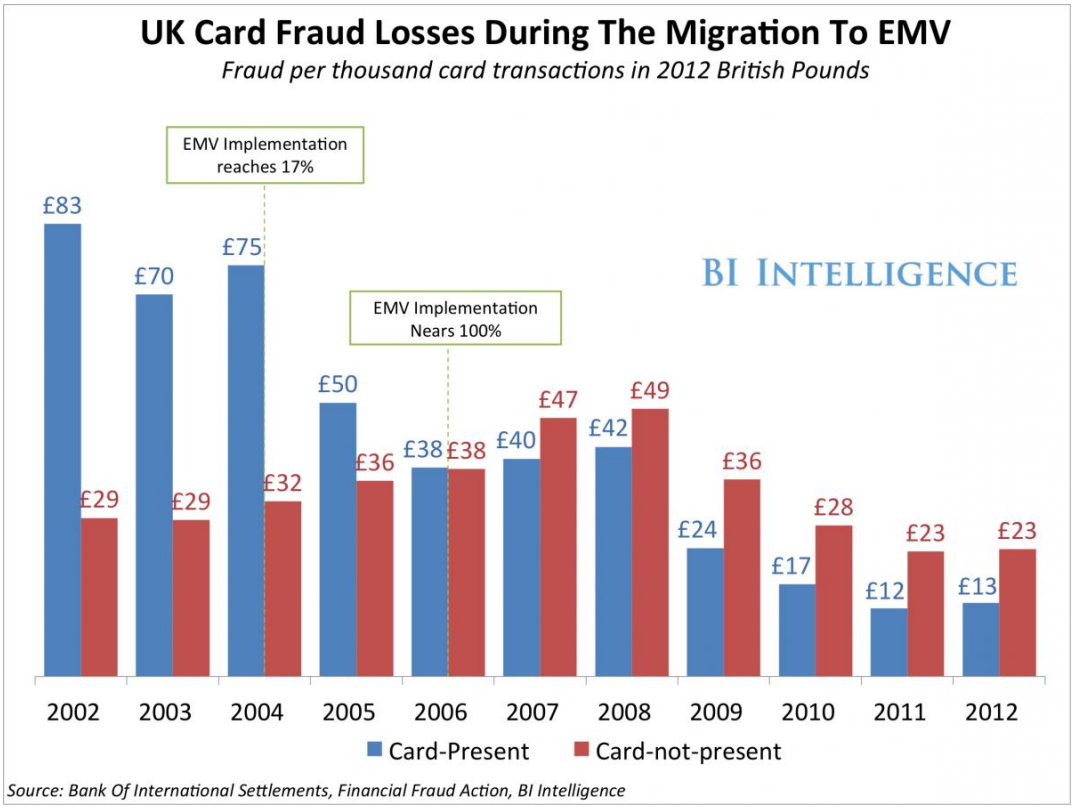
Dynamic cryptograms are essentially encrypted codes that change with every transaction. The cryptogram is sent through the merchant's payment terminal to the processor and then to the issuing bank, which decrypts the cryptogram with a private key and authorizes the transaction. Private keys refer to a function held by a single entity, in this case the processor, that is used to decrypt an associated encrypted set of values. The cryptogram is used to confirm that a transaction came from the appropriate card, and only the card issuer, which holds the private key, can make that authorization. *(Note: This is a very simplified version of how EMV works. There are numerous other ways EMV transactions are authenticated depending on the type of transaction and how it is transmitted.)*

- In combination with the added risk-assessment capabilities of EMV cards, dynamic cryptograms make it difficult for fraudsters to make counterfeit cards. While fraudsters can still steal the card number (PAN) and other sensitive data from the merchant's systems or from somewhere else along the transaction chain because this data is not encrypted, they cannot easily manufacturer a counterfeit card that will generate usable cryptograms.

- In addition, depending on how EMV is implemented, it sometimes requires PIN entry to complete transactions. This makes it even more difficult for criminals to use stolen cards, because they would typically not know a person's PIN. The chip-and-PIN EMV standard is used in the UK, though the US seems likely to adopt the less secure but faster chip-and-sign standard.

EMV is very good at reducing in-store card fraud but ineffective at mitigating online fraud. The insertion of a card into a payment terminal is what initiates the transmission of a dynamic cryptogram. Without this insertion, which is not conducted in online transactions, there is limited security in place to keep fraudsters from using data stolen from EMV cards to commit fraud online.

In keeping with this, EMV cards did reduce in-store fraud when the security standard was implemented in the UK and other parts of the world. However, fraud quickly moved to online channels.



Encryption

As EMV is implemented in the US, the sensitive data that is transmitted during an EMV transaction will remain a target for criminals who can continue to use it at remaining magnetic stripe terminals. In addition, as online merchants are increasingly targeted, they will need to improve the security of their systems to avoid breaches. So the question then becomes how payments companies can secure that data to keep it from being accessed in the first place.

There are two ways to protect any sensitive data, in this case payments data.

- The first is to fortify sensitive data so it is difficult to access. But this strategy has proved ineffective at the consumer/merchant level. Target, Home Depot, and other retailers that suffered data breaches in 2013 and 2014 all had systems in place to make it as difficult as possible to access the merchant systems that house payments data. Fraudsters still seem to find ways in under this type of system, though. For example, someone could gain administrator access to the system. Card numbers are accessible there and can be stolen.
- The second strategy is to degrade the data so it is not easily usable if it is stolen. Encryption is a common way to degrade data.

Encryption has been used by the card networks during payment processing for years. But it is beginning to be implemented at the payment terminal because this is where data is most vulnerable, as mentioned above. Brick-and-mortar and online merchants are beginning to choose payment solutions that encrypt data as soon as it enters the payments chain. There are many different types of encryption for payments data, but in all cases card data is translated into new values, with each transaction using a digital "key," or algorithm.

Essentially, a string of data is translated into a new string, which can then be decrypted for authorization purposes further along the payments chain. The benefit of encryption is that should fraudsters access the merchant's systems or the systems of another player in the payments chain, any data they steal will be

essentially useless. A fraudster would have to gain access to the corresponding digital key to unlock encrypted values for the data to be useful for conducting fraudulent transactions. As for accessing decryption keys, this is something that is very difficult to do, as we'll discuss further on.

Point-to-point encryption — a subset within end-to-end encryption

End-to-end encryption (E2EE) is a blanket term for solutions that encrypt sensitive data at each of the different points within the payments chain. An E2EE implementation encrypts data from the time the card is dipped into a specially designed card-encrypting payment terminal to the time it reaches the merchant's card processor.

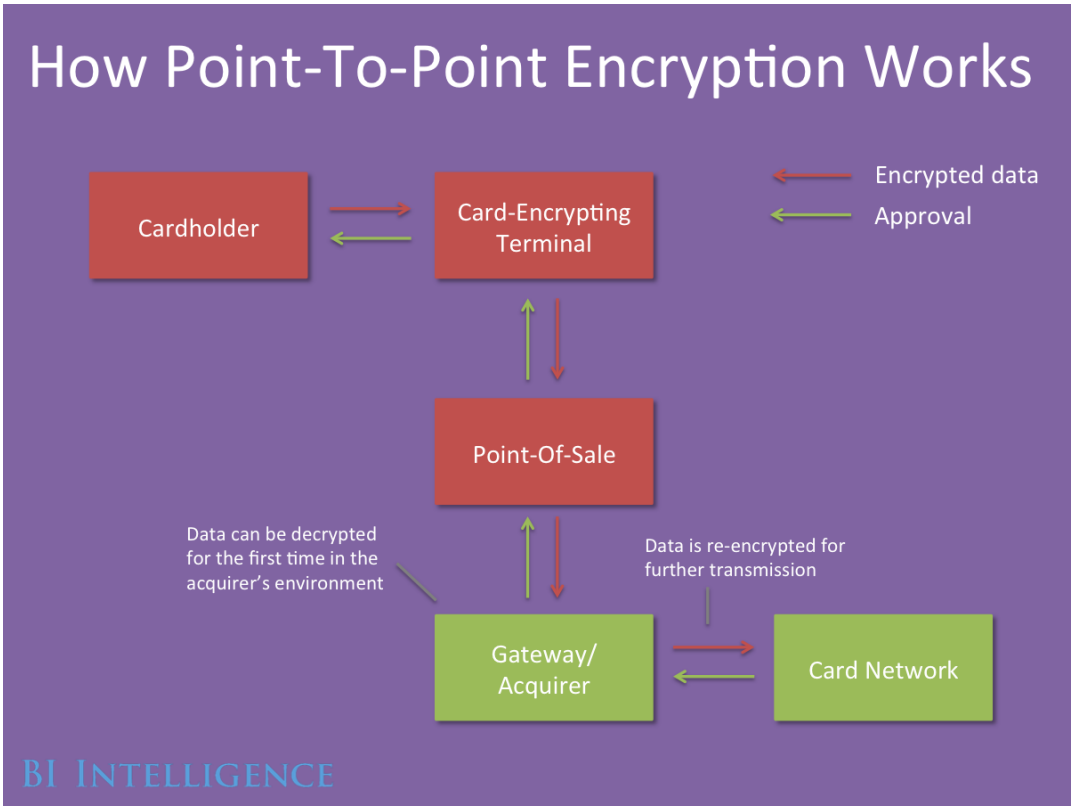
Typical E2EE solutions are most applicable to offline environments and are subject to full Payment Card Industry (PCI) compliance requirements. PCI compliance is an industry-standard setting body for data security.

A type of E2EE called point-to-point encryption (P2PE) is primarily for merchants with physical payment terminals, typically brick-and-mortar retailers. It is highly secure in that encryption at each point in the chain — from the point of interaction (where card data enters the system) until it reaches the processor — is clearly defined and subject to specific requirements, including that decryption keys are not managed or possessed by the merchant. (With E2EE, decryption keys may be managed by the merchant.)

P2PE is different from E2EE in that merchants that have adopted the solution are exempt from many of the more burdensome aspects of PCI compliance. For large retailers a Qualified Security Assessor is still required to check the merchant's systems, but the scope of assessment is reduced from about 300 requirements to about 30. That means retailers that adopt this form of security will most likely pay less in assessment costs.

Only a handful of US payment service companies offer PCI-validated P2PE systems, the first of which was Bluefin. P2PE isn't necessarily better than every E2EE solution, but it is more tightly defined, hence the PCI compliance exemptions.

For this report, we'll use P2PE to illustrate E2EE.



According to the PCI, P2PE can use numerous encryption methods. The most widely implemented is symmetrical encryption with Derived Unique Key Per Transaction (DUKPT) key management.

DUKPT is complex, but in a nutshell, a unique master key is injected into each tamperproof payment terminal. The processor that receives the transaction has the unique master key as well. A master key generates subkeys that both encrypt and decrypt data. When a transaction is made at the payment terminal, the master key creates a unique subkey that then encrypts the data from that

transaction. The transaction then makes its way through the merchants system and on to the acquirer.

To allow the acquirer to unlock the data correctly, the encrypted transaction includes a unique key identifier — the equivalent of a serial number. When encrypted data gets to the acquirer this serial number is used to identify what subkey should be used to decrypt the data. For the transaction to be completed the data is re-encrypted and passed to the card network for another round of decryption and approval.

This type of encryption disincentivizes fraudsters from attacking merchants for three reasons:

- Obtaining the key for a particular transaction allows the fraudster to decrypt the payments data associated with only that one transaction. This increases the risk and reduces the reward of data theft. Because fraudsters try to gain data from a lot of different cards at once, which can then be sold online to different criminal networks, there is little payoff to going after a single unique key.
- Obtaining the master key, which generates unique keys, is extremely difficult. Payment terminals are designed to erase the master key if the terminals are tampered with by physical means. There are few access points to obtain master keys on the processor side, and they are well guarded.
- The master key is unique for each terminal, so obtaining one would allow the attacker to access the transaction data for only that terminal.

It's important to note that encrypted data is still considered sensitive in all cases except in PCI-validated P2PE security protocols, so security systems without P2PE encryption still retain some of the PCI compliance burden.

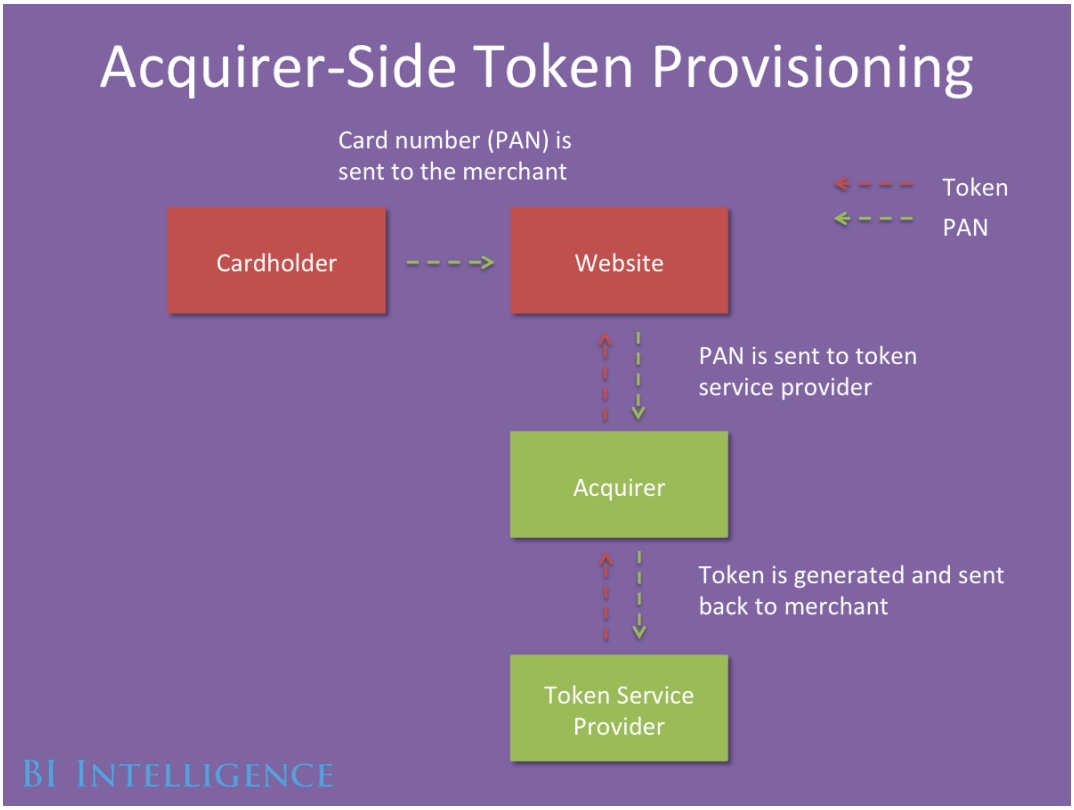
Acquirer-side tokenization

Another type of payment security is called tokenization. Similar to encryption, there are multiple types of tokenization. We'll look at acquirer-side tokenization first. This is the most widely used form of tokenization and is provided by acquirers or processors. It is primarily aimed at e-commerce merchants.

Tokenization is attractive to e-commerce merchants because it can be used to lower shopping-cart abandonment rates while still removing sensitive data from the merchant's environment and putting the merchant at lower risk of fraud.

How acquirer-side tokenization works

Entering card information is arduous, and in the 30 seconds it takes to fill out those details on the purchase page of an e-commerce site, a potential customer might decide to close his or her window and abandon the purchase. So merchants will sometimes opt to store a customer's card information so the customer will not have to go through the process of re-entering information during future purchases.



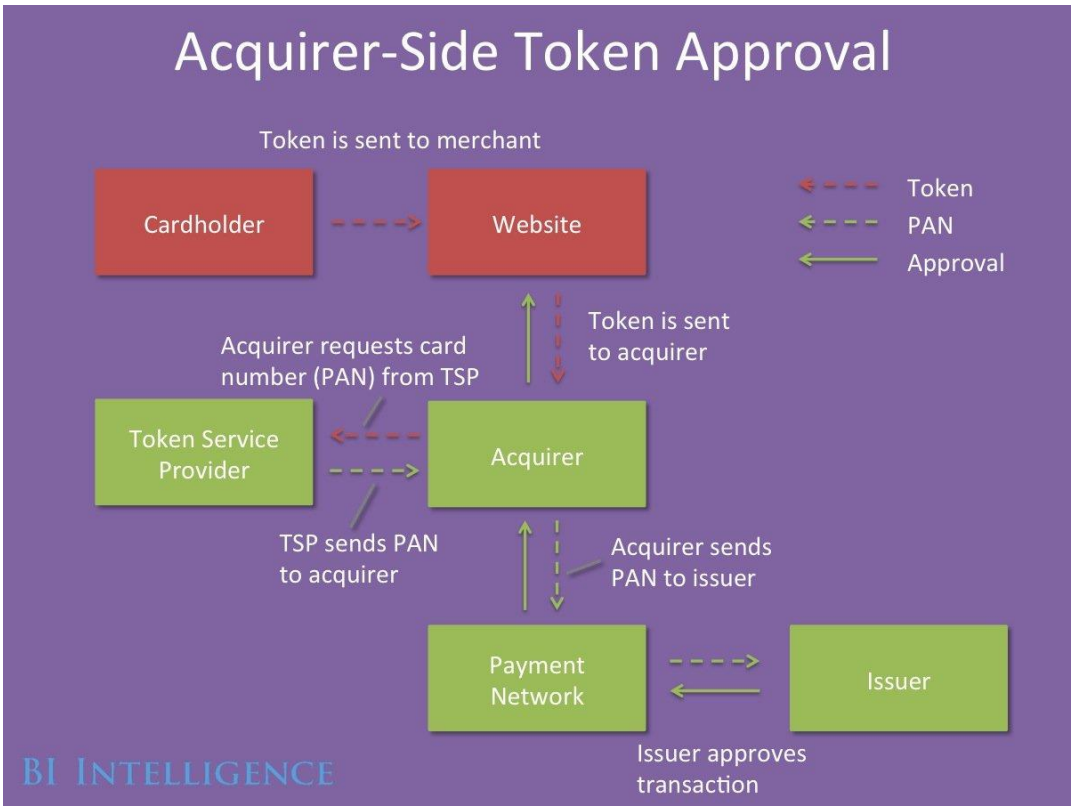
But storing card information introduces a new problem for merchants. If an e-commerce merchant has lots of card information on file, that merchant becomes a target for hackers. And if hackers are successful in obtaining the data, then the merchant will most likely be liable for the costs associated with the breach.

Acquirer-side tokenization allows repeat customers to make purchases without having to re-enter card information while at the same time removing sensitive information from the merchant's environment.

In an acquirer-side tokenization scheme, a gateway provider or processor such as Braintree or First Data offers to take an online merchant's card data and replace it with tokens. Tokens are randomly generated values assigned to each card. In an initial transaction, card data is transmitted from the merchant to an acquirer or token service provider (TSP). The acquirer or TSP then turns this data into a token, which is then passed back to a merchant and stored for future transactions.

The sensitive card data remains stored by the acquirer or token service provider in a secure digital token vault.

The next time a customer comes to the merchant's website, he or she opts to use the stored card to pay. At this point the token associated with the card is sent from the merchant through the processing chain to whoever issued the token. It is then exchanged for the original card data, and that card data is sent to the card network for further processing.

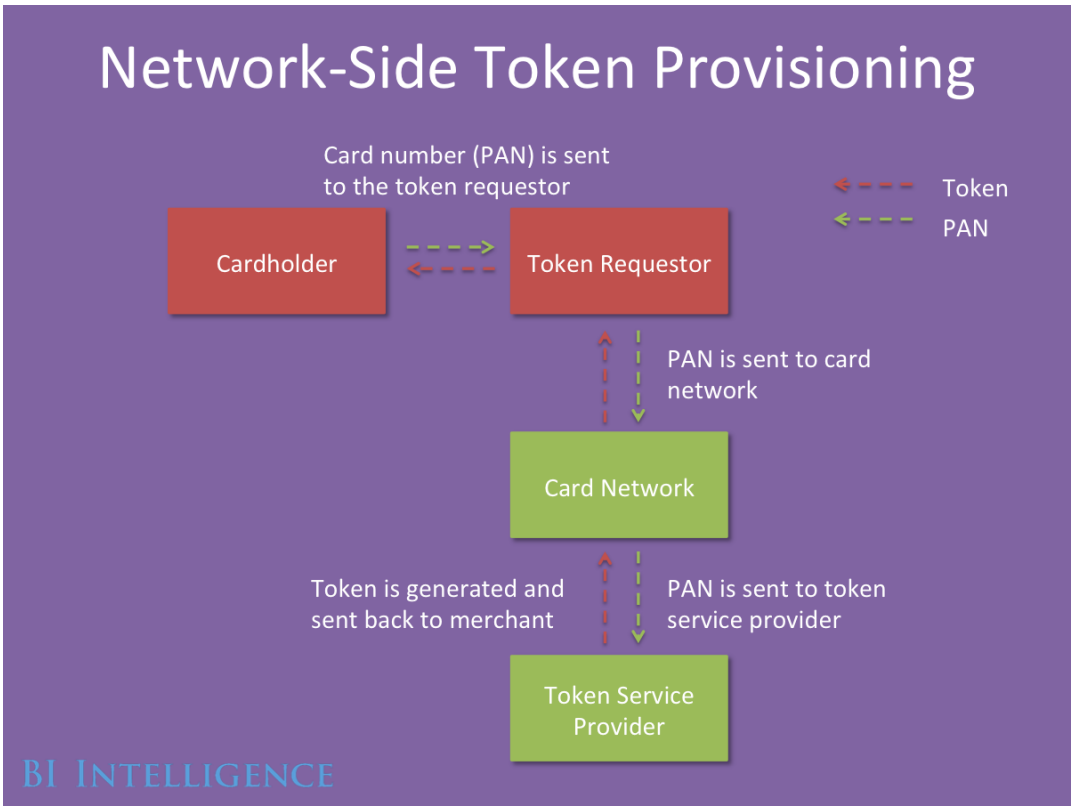


Unlike with encryption, an algorithm (called a key) is not used to translate a card number into a token value. There is no logical relationship between the token and the original payment data. As a result, there is no way to get back to the original card number without a ledger of paired values from the digital token vault. Merchants are only housing tokens in their systems, and if the tokens are stolen, they can't be used to make a purchase on another website. As a result, the merchant is highly protected against breaches.

In contrast, because encrypted values are reversible they can eventually be hacked — it just takes a long time and lots of computing power. This means there are numerous advantages to tokenizing data when possible.

Of course, when a customer makes a transaction on a website for the first time, sensitive data *is* transmitted and could still be stolen because it has not yet been tokenized. For this reason, merchants must still consider encrypting data in addition to implementing acquirer-side tokenization. First Data's TransArmor security solution, for example, both encrypts data and tokenizes it.

Network-side tokenization



Network-side tokenization is the newest form of tokenization to be implemented. It is used mainly for transactions made via mobile devices, and it is the system used by Apple Pay.

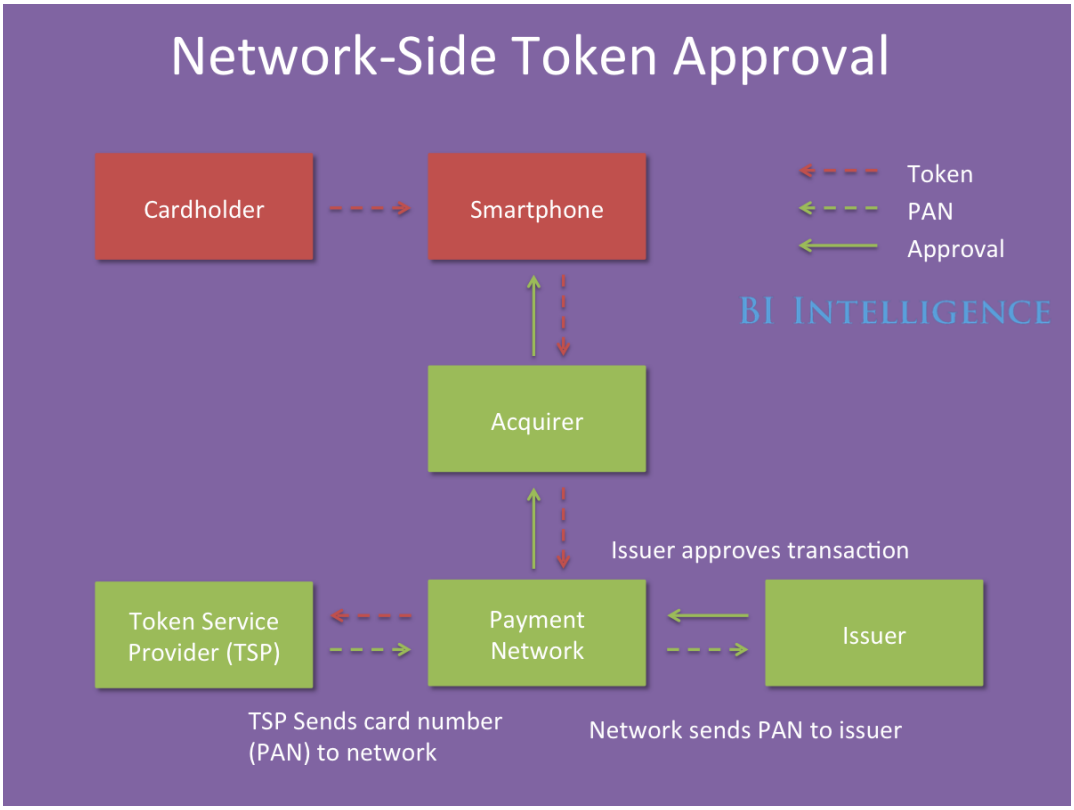
We'll use Apple Pay as an example of how this type of tokenization works.

When a cardholder enters his or her card data into Apple Pay on an iPhone 6 for making future purchases, Apple receives the data. But Apple does not want to keep that data in its environment because it presents a huge liability. To avoid the liability but allow the customer to enter payment info only once, Apple sends that card data to a card network or some other token service provider (TSP). Today the major card networks are the TSPs for Apple Pay, though others in the payments chain or a standalone TSP could emerge and offer network-side tokenization.

As with acquirer-side tokenization, the TSP assigns a unique random value to the PAN. The new token looks like a normal PAN and is stored within the secure element of the user's iPhone for use in online or in-store Apple Pay transactions.

The token can be accepted by processors at multiple merchants because it is formatted as an ordinary card number. (Acquirer-side tokens can be used at only a single merchant.) With network-side tokenization, a new token does not need to be created each time a consumer pays using Apple Pay at a new merchant. All processors working with all Apple Pay merchants can accept the original token's format and send the token through the payments chain until it reaches the TSP for approval.

The PAN is then retrieved by the TSP and sent to the issuer to approve the transaction.

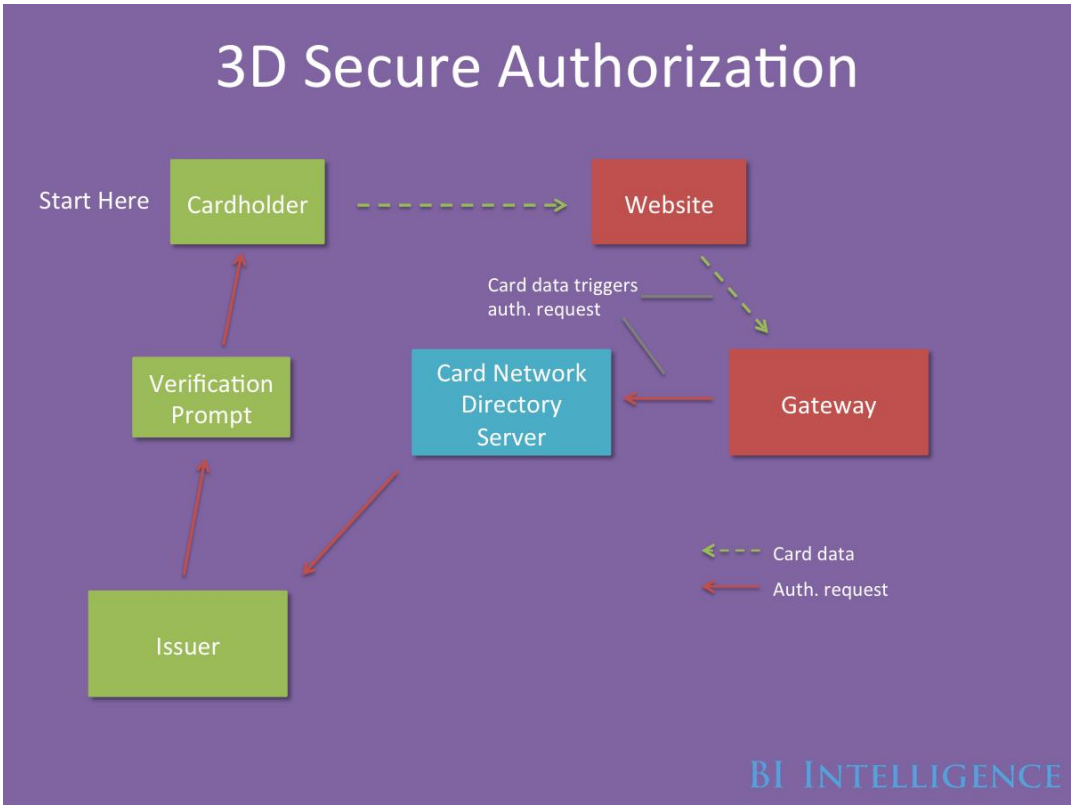


Soon more payments companies working across multiple merchants will look to adopt network-side tokenization. For example, Samsung Pay, the coming payments feature for Samsung's S6, will use network-side tokenization.

In addition to the security that comes with tokens, the data sent to the merchant using Apple Pay includes a dynamic encrypted identification number so that even if the token is stolen, it can't easily be ported onto magnetic-stripe cards and used for fraudulent transactions. That's because the network would recognize that the transaction lacks the necessary ID and is not coming from the device associated with the token.

One major advantage of network-side tokenization is that sensitive data must be transmitted just once for a token to be issued that can be used at multiple merchants. That greatly reduces the likelihood that someone will be able to steal that data, because fewer initial transmissions means fewer opportunities for theft.

3D Secure



3D Secure is another security protocol specifically aimed at online transactions. This type of security solution allows the merchant to authenticate the user even in an online environment.

While online merchants have solutions for authenticating card data, they often lack a way to authenticate who is using that data. Even if a merchant has an adequate way of protecting data in transmission and storage, it has no way to verify that the user is the person who owns the card.

This creates two opportunities for fraud.

- First, the card number can still be stolen either through physical card theft or a data breach of a merchant without adequate data protections. That card data can then be used online at a different

merchant's e-commerce platform, and the e-commerce merchant would most often be responsible for bearing the cost of fraudulent purchases.

- Second, the cardholder can commit "friendly fraud," meaning the cardholder makes a purchase and then claims that the purchase was fraudulent, resulting in a chargeback for the merchant. If the cardholder were authenticated at the time of purchase, he or she would not be able to as easily later claim it was a fraudulent purchase.

3D Secure systems like Verified by Visa and MasterCard SecureCode aim to solve this problem by authenticating the user in addition to the card data. The security solution is usually offered by the merchant's acquirer or gateway provider and is named for the three domains it was designed to protect: the acquirer's domain, the issuer's domain, and the network that connects them.

3D Secure verification prompt.

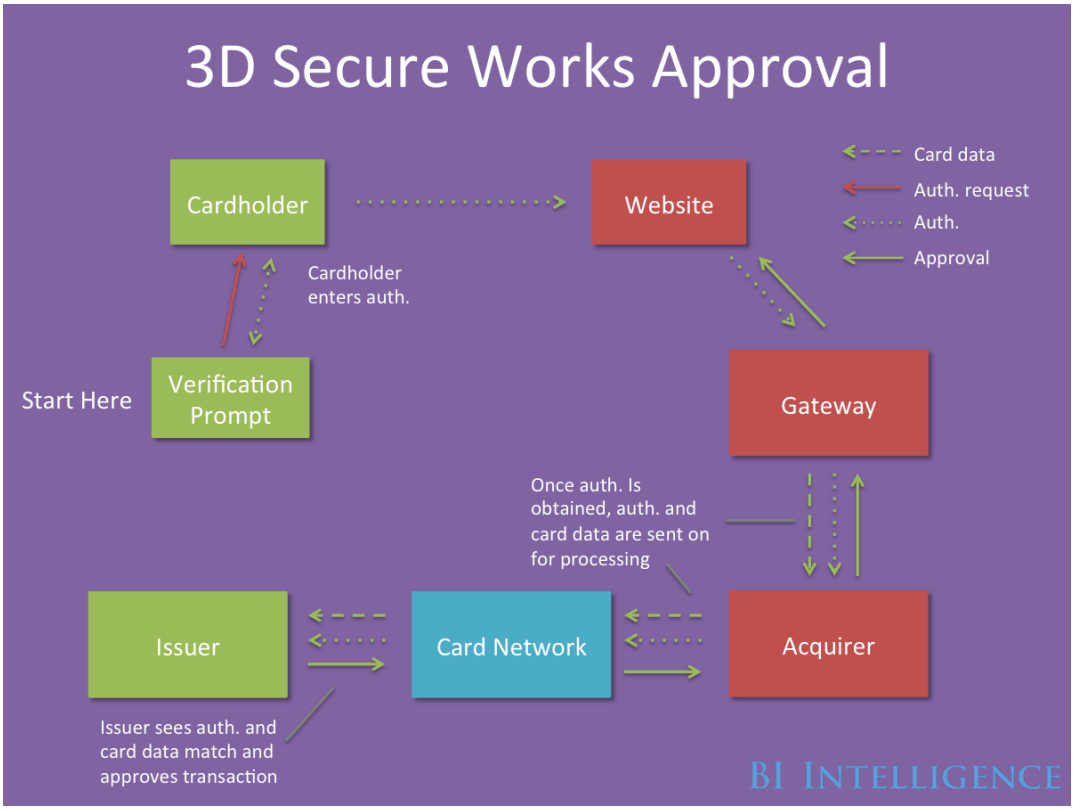
In transactions with merchants that use 3D Secure, not every consumer is prompted to go through this additional security mechanism. Someone might be flagged for additional authentication if a purchase is coming from a foreign country or if an account has a lot of chargebacks on it.

Here's how 3D Secure works:

When a consumer goes to make his or her first purchase at a merchant, the card data is sent to the gateway, which triggers a prompt within a window hosted by the issuing bank asking the consumer to register for 3D Secure. The consumer then provides his or her account credentials and bank password or some other additional identification. (In coming versions of 3D Secure, biometric authentication or a two-factor authentication code will be used instead of a bank password.) The next time the consumer makes a purchase with this merchant,

the consumer will again be prompted to enter identifying credentials in an inline frame or pop-up window, though registration is no longer necessary.

Passcode or additional data entry helps the issuing bank confirm that the person using the card data is actually the cardholder because the cardholder is more likely to be the only one in possession of their bank password, biometric data, or mobile device to which a one-time use code is sent. Once authenticated, the card data and the user authentication leaves the gateway and travels through the acquirer and then through the rest of the processing chain for approval, as displayed below.



While 3D Secure does provide added security, it also has numerous downsides:

- A fraudster could steal card data through typical means and enter it into a site using 3D Secure verification. Assuming the consumer whose data has been stolen has not set up a 3D Secure account already, the fraudster with additional personal details like the consumer's bank password could

register for 3D Secure using the real consumer card and a fraudster's own biometric data or mobile phone number. The fraudster would then have a 3D Secure account that could be used until the fraud were identified. This is akin to carrying out identity theft.

- Some merchants don't like it because it is a nuisance to customers to enter more information every time they make a purchase, and it can often lead to shopping cart abandonment.
- Because additional authentication takes place in a pop-up window, it creates an opportunity for phishing scams. A hacker could create a window that looks like a 3D Secure prompt and get consumers to enter bank account passwords. Inline frames will be used instead of pop-up windows in the newest version of 3D Secure to solve this problem.

On the other hand, implementing 3D Secure shifts the burden of fraud from the merchant to the card issuer, which is a significant incentive for merchants with high fraud losses. That is because the issuer is responsible for user authentication in addition to data authentication, so if fraud occurs, the card issuer must bear the cost.

3D secure is typically used by smaller merchants because they have weaker analytics for detecting that the appropriate person is using a card. For example, their systems may not flag a transaction from a card issued in the US with a shipment address in the Ivory Coast. These merchants bear enough of a burden from fraud costs that they are less concerned about shopping-cart abandonment.

THE BOTTOM LINE

- In 2014, fraud cost US retailers $32 billion, about half of which was perpetrated using compromised payment-card accounts.
- EMV will help mitigate in-store fraud, but fraud will then move to online channels.
- Encrypting sensitive payment data from the point of capture makes it much more difficult for fraudsters to harvest usable data from in-store and online transactions.
- When payment data is tokenized, it is effectively impossible for hackers to access the sensitive data from an online merchant's environment because there is no logical relationship between the payments data and the token. It removes sensitive data from the merchant and the processor's environment, but the cardholder still does not need to re-enter payment credentials with every purchase.
- 3D Secure is an imperfect answer to online user authentication. Merchants that implement 3D Secure gain an added layer of user authentication but at the same time risk higher shopping-cart abandonment.

About BI Intelligence
BI Intelligence, a research service from Business Insider, brings you and your team business intelligence for the digital age. Our research is fast and nimble, reflecting the speed of change in today's business. We give you actionable insights that enable smarter and better-informed decision-making. We publish in-depth reports, news, and an exhaustive library of charts and data focusing on key digital areas: mobile, social, e-commerce, digital video, payments and more.
To learn more please visit: intelligence.businessinsider.com.

Analysts
BI Intelligence has an experienced team of analysts led by Henry Blodget, CEO & Editor-in-Chief of Business Insider. BI Intelligence's team of dedicated analysts have deep analytical and industry experience, and work with Business Insider's journalists covering specific verticals, such as technology, advertising, and strategy, to produce unique insight and analysis on today's digital trends.