Tokenization

With the holidays quickly approaching, many retailers are increasing their fraud and risk management efforts to prevent a repeat of the events that occurred last year. Fraudulent transactions pose a risk to merchants; however, a truly serious risk lies in merchants' potentially vulnerable customer data. As data travels through the merchant's system to the processor and back, it can be exposed and become vulnerable to criminal interception. Criminals can hijack lucrative data sell it to fraud rings, resulting in stolen consumer identities and bruised reputations for merchants.

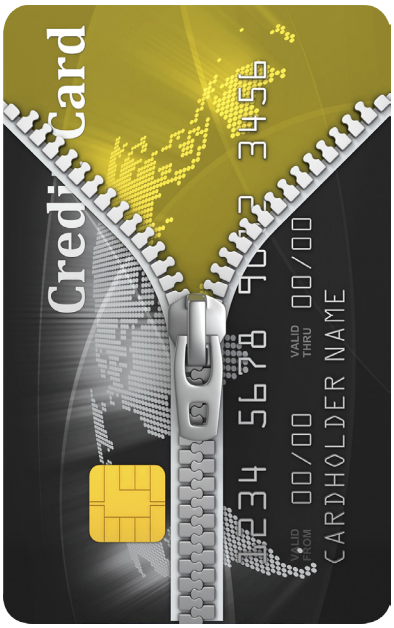


Illustration of the problem: Target data breach by the numbers

In November of last year, shrewd criminals looking for payment card data breached Target's POS system. The hackers responsible for the Target breach garnered an estimated **$53.7 million** in income after selling roughly 2 million of the stolen cards, which sold at a median price of $26.85 each.[1] Other losses incurred include:

- **40 million** stolen credit and debit cards[2]
- **70 million** Target records stolen with name, address, email address and phone numbers[3]
- **46%** drop in profits for Target during the fourth quarter of 2013 compared to the year prior[4]
- **$200 million** cost to community banks and credit unions to reissue roughly half of the cards stolen in the breach (~21.8 million cards).[5]
- **$18.00 – $35.70** price per card that was stolen and resold on the black market[6]
- **1 million – 3 million** cards were stolen, successfully sold on the black market and used for fraud.[7]

Target was not the first or the last of these mega breaches. More recently, Home Depot fell victim to fraudsters that were able to hack in and steal data, affecting more than 56 million payment cards total.[8] Since the breach was first reported in early September, the number of stolen cards available for sale on black market websites has soared from 52,000 to roughly 100,000 as the thieves increase the inventory.

Home Depot fell victim to fraudsters that were able to hack in and steal data, affecting more than 56 million payment cards total.[8]

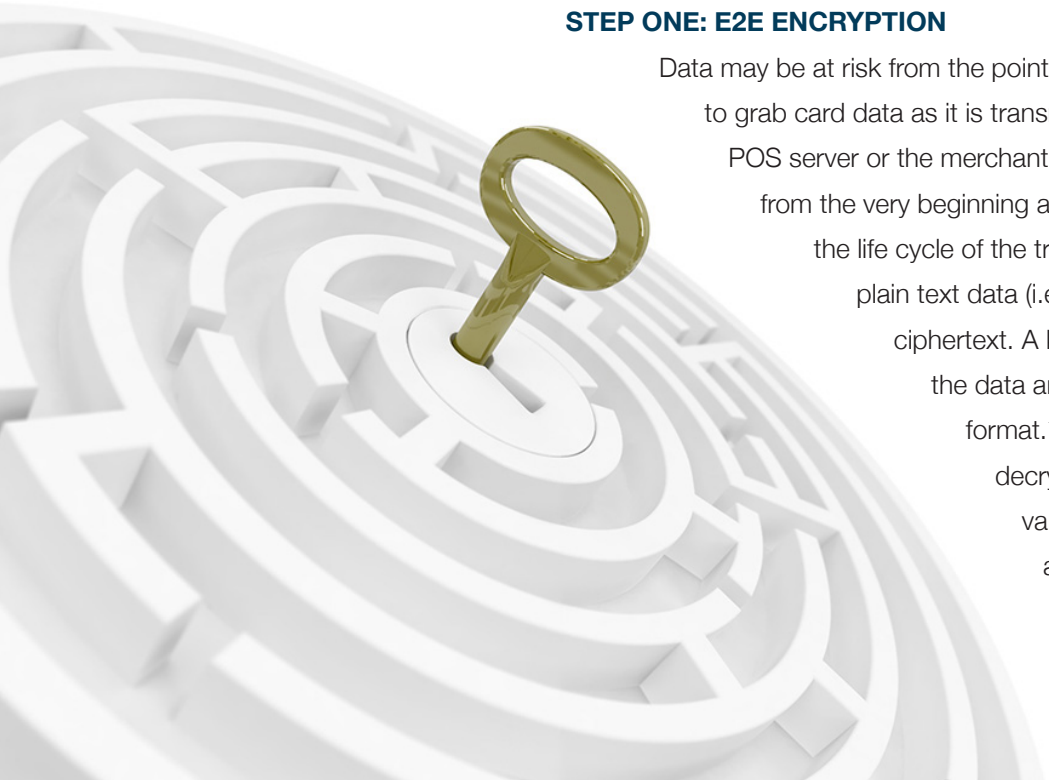
Security matters to consumers and you can't put a price tag on peace of mind. 58% of customers have expressed "deep concerns" about their personal data in online transactions[9] and roughly one out of three identity fraud victims will avoid particular merchants in the future.[10] Cleaning up the mess from any breach is expensive and the reputational damage alone can cost merchants millions.

Tokenization as a Solution

Tokenization substitutes sensitive data with a non-sensitive "token" that cannot be exploited by fraudsters. This allows merchants to be PCI compliant – a requirement for all merchants that accept credit cards to safeguard valuable consumer data – with added convenience and can be paired with additional security tools and tactics to enhance other security efforts.

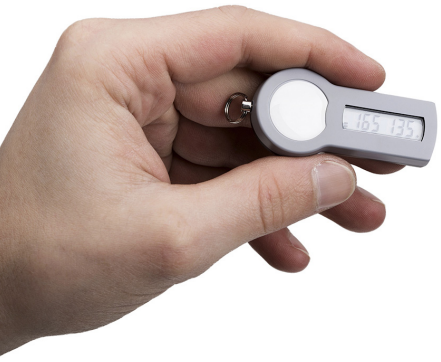
By replacing consumers' payment card data with a software token that acts as a proxy during most of the payment process, customer data is protected from possible theft and fraudulent use. Card information entered by the shopper is encrypted and sent directly to the processor where it is decrypted and sent to the customer's issuing bank to be authorized through a secure connection. The acceptance or denial code is then sent from the processor to the merchant with a token that the merchant can store in case a dispute arises in the future.[11] The token acts as a substitute for the card number, rendering it useless to criminals that may intercept it because no way of mapping that token to the original card number.

Tokenization is part of a two-step solution



STEP ONE: E2E ENCRYPTION

Data may be at risk from the point-of-capture and it is possible for a criminal to grab card data as it is transmitted in plain text from a card reader to the POS server or the merchant's central server.[12] Encryption protects data from the very beginning and maintains data protection throughout the life cycle of the transaction by using algorithms to convert plain text data (i.e. the PAN) into non-readable text called ciphertext. A key or algorithm is then used to decrypt the data and convert it back to the original plain text format.[13] The master key used to encrypt and decrypt data is safely stored in the processor's vault. The actual transmission path of the data along the network can be encypted as well to further reduce a merchant's risk.[14]



Possible Points-of-Capture Where Data Becomes Vulnerable[15]

- Manual entry of card data into a terminal (sales clerk entering card info into in-store POS system)
- Manual entry of card data into a web-based form (ecommerce)
- Swipe of a magstripe card
- Insertion or tap of a chip-enabled payment card or instrument

STEP TWO: TOKENIZATION[16]

During the transaction, the PAN is sent to a "vault" – a highly secure server and PCI-compliant environment. Tokenization occurs when a random, unique "token" is returned to the merchant rather than live credit card data in the authorization response. A secure reference table or master key is created to allow authorized look-up of the original PAN with the token as the index. This surrogate value assigned to the sensitive data preserves the value of the data for the merchant while removing the risk that thieves can steal it and use for nefarious purposes. The token value is completely meaningless without access to the master key and cannot be used in any type of transaction.[17]

The token has value to the merchant and can be used just like the original card number for operational purposes like returns, sales reports, marketing analysis and recurring payments but it cannot be used outside of the merchant environment to purport fraud.

Tokenization supports compliance requirements

Tokenization can significantly reduce PCI scope for merchants tasked with protecting stored credit card data because it eliminates the need to actually store card data.

Strong encryption of electronically stored cardholder data is mandated by PCI-DSS guidelines. The cost of encryption can become burdensome for companies that have thousands of customers' worth of cardholder data to protect. Additionally, the encrypted values tend to take up more memory in databases than the original data, creating burdensome storage expenses. Industry reports indicate that costs can balloon to as much as $6 per customer to encrypt data for organizations with 100,000 or more customers.[18]

On-site electronic storage of encrypted data poses its own risks, including the possibility that thieves will intercept the encrypted files. These criminals can "reverse engineer" the encryption key and decode the encrypted files for criminal gain.[19] Tokenization adds a layer of protection that cannot be violated because of the unique surrogate value assigned to each card number. No mathematical formula is used to generate these random surrogate values, so they cannot be reverse engineered. The original card data is stored off-site in a high security storage facility and while the merchant can use the token for day-to-day customer interaction, it never has the original card number in its possession again after the initial tokenization.[20]

Companies – especially those with large customer databases – stand to save a lot of time and money by utilizing tokenization. The off-site storage of data eliminates the PCI DSS requirement of network scans since the merchant is not holding any cardholder data that requires protection. Additionally, tokenization reduces or eliminates the cost of encryption software and the subsequent system memory requirements.[21] Finally, the peace of mind both to merchant and consumer regarding the security of sensitive data is priceless.

Tokenization is a big step in the right direction, but it is not a silver bullet; merchants still need comprehensive layered protection in place to guard against all types of fraud perpetrated by shrewd, dynamic criminals that are constantly evolving. Tokenization is a highly effective method of protecting cardholder data but it won't stop criminals from trying to commit identity or other fraud. Merchants should fortify front-end fraud prevention with additional tools across the entire transaction life cycle to ensure comprehensive fraud prevention and management is in place to protect payments and boost profits.

Tokenization reduces or eliminates the cost of encryption software and the subsequent system memory requirements.[21]

ABOUT VERIFI

Since 2005, Verifi has helped merchants protect their payments and boost profits. Offering a wide-range of flexible, configurable fraud prevention and chargeback management tools, Verifi makes it easy to prevent and fight payment disputes, protect the entire transaction lifecycle and increase revenue. Verifi is PCI Level 1 certified and headquartered in Los Angeles, California.

VERIFI™

For More Information

Main Phone: (323) 655-5789 Mon-Fri 8:00 AM – 5:00 PM PST
Main Fax: (323) 655-5537
Email Address: info@verifi.com

Mailing Address: 8391 Beverly Blvd., Box #310, Los Angeles, CA 90048

Citations

1 *http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/*

2 *http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/*

3 *http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/*

4 *http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/*

5 *http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/*

6 *http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/*

7 *http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/*

8 *http://www.wcsh6.com/story/news/local/2014/09/18/home-depot-data-breach-grows-worse-for-mainers/15833845/*

9 *http://cardnotpresent.com/news/cnp-news-jan14/Report__U_S__Consumers_'Concerned'_about_Breaches,_But_Not_Showing_It_-_Jan__30,_2014/*

10 *http://www.lexisnexis.com/risk/insights/true-cost-fraud.aspx*

11 *http://www.internetretailer.com/2014/03/03/sponsored-special-report-staying-one-step-ahead-criminals*

12 *http://files.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF*

13 *http://files.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF*

14 *http://files.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF*

15 *http://files.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF*

16 *http://files.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF*

17 *http://files.firstdata.com/downloads/thought-leadership/EMV-Encrypt-Tokenization-WP.PDF*

18 *http://blog.pcifree.com/24/tokenization-eases-burden-of-data-security-for-pci-compliance/*

19 *http://blog.pcifree.com/24/tokenization-eases-burden-of-data-security-for-pci-compliance/*

20 *http://blog.pcifree.com/24/tokenization-eases-burden-of-data-security-for-pci-compliance/*

21 *http://blog.pcifree.com/24/tokenization-eases-burden-of-data-security-for-pci-compliance/*