Century Business Solutions

2014

An Argument for Tokenized Electronic Payment Systems

Century Business Solutions
20 Pacifica Suite 1450, Irvine CA 92618
Phone: 888-500-7798
Fax: 888-500-7797

Century™
BUSINESS SOLUTIONS

Contents

Report body

Supplementary graphs

Introduction: The Reason Your Business Needs a Tokenized Electronic Payment Solution—Yesterday

In today's age of consumers relying more heavily on intangible credit than physical cash, it's no coincidence that credit card fraud across the United States has skyrocketed. The stories of high-profile data breaches like those of Target, Neiman Marcus, Home Depot, and TJ Maxx, enter the collective consciousness much more quickly and stay there for much longer thanks to the internet, making some business owners afraid to accept credit card payments online—or, to accept credit card payments at all.

Fortunately, the technology of tokenization, long employed by institutions in various capacities specifically to combat fraud, has now been digitized to protect sensitive credit card data, creating a digital wall of security that is virtually impervious to hackers. This new layer of security should detract from card-not-present fraud substantially in the coming years as its popularity grows among businesses.

Tokenization is a relatively new player in the data security world, but because of its low cost to implement and extremely potent security advantage, Century Business Solutions recommends a tokenized payment processing solution to any business, no matter the size or industry.

DONT BE NEXT.
CREDIT CARD DATA BREACHES HAPPEN EVERY DAY.
PROTECT YOUR BUSINESS WITH THE POWER OF TOKENIZATION
HACKED
THE WORLD
YOUR NUMBER ONE SOURCE FOR HEADLINES
Since 1883
COSTLY DATA BREACH SLAMS
YOUR BUSINESS
Countless customers
lawsuit pending
Stock price drops

How tokenization works

Tokenization essentially turns a static piece of information—a credit card number and other associated data—into a dynamic one so it is only accessible by a gateway that can read the associated token. Dynamic in this case means *changing*, so the numerical or character value of the token can be set to expire or change at any time, rendering the data all the more useless to an outsider. For example, whereas before a hacker could simply infiltrate a mainframe computer and access different static—*unchanged*—credit card numbers, a hacker looking at a series of credit card tokens would see something completely meaningless, unrelated at all to physical credit card numbers. A tokenized gateway is equipped to understand the tokens—and, of course, controls how often the tokens expire and change—so a hacker would need access to both of these in order to steal any sensitive information.

Findings: Tokenization in its digital form isn't free, but it can save businesses real money, not to mention countless hours of stress and reconciliation

Though the idea of tokenization had its advent during the dawn of the world's first currencies—when less valuable objects or goods were used in trade to prevent the loss of their more valuable counterparts like gold and other precious materials—it hadn't been employed in the digital realm until 2010 when it was pioneered by Heartland Payment Systems following a breach of Heartland's own network.[6] Since then, payment processors have rushed to develop their own tokenization technologies in an effort to stay relevant, and this development has come at the expense of the processors as a growing number of businesses demand the technology for their own use. Now that the technology is widely available, business owners ought to seriously consider taking advantage of it regardless of any initial cost difference for the sheer security potential, analogous to a home alarm system or auto insurance. There were several high-profile data breaches in 2013, in which massive companies were held liable for mind-blowing numbers of stolen data records.

Neiman Marcus had 530,000 compromised in just four months.[1] Target's data beach encompassed 40 million customer records[2] and reportedly cost the company $148 million.[3] Home Depot's saw an even more staggering 56 million records stolen.[3] And, in 2007, TJ Maxx fared the worst of the highly-publicized accounts, having seen an astonishing 94 million customer records stolen.[4] **(See Figure 1.)** If these larger-than-life companies had utilized tokenization technology, fraudsters could have hacked all the way into their mainframes and still would have been unable to make sense of the credit card tokens they would have acquired. Thus, a triflingly small adjustment like this could have prevented many hours of pain and the loss of many millions of dollars. **(See Figure 2.)**

How does tokenization change a business' sales process?

Implementing a tokenized gateway will not affect the sales process of a business using an online virtual gateway or an ERP software integration, since the tokenization itself is completely computerized. Businesses using physical credit card readers—ones not tied into a computer system—will need to upgrade to virtual gateways in order to take advantage of a tokenized solution. In many cases virtual gateways provide other benefits to users, such as native reporting tools and transaction history lookup features, which will perhaps provide more of an impetus to change procedures than increased security alone.

Specifically, whereas non-tokenized businesses conduct transactions using a physical card terminal connected to a telephone line, tokenized businesses use a virtual gateway to enter a customer's card information directly into a computer, whether manually keyed in or swiped through a card reader or POS system. The gateway user never sees the actual tokenization process, so virtual gateway and integrated POS users would not see a substantial difference in their procedures by upgrading from a non-tokenized gateway to a tokenized one.

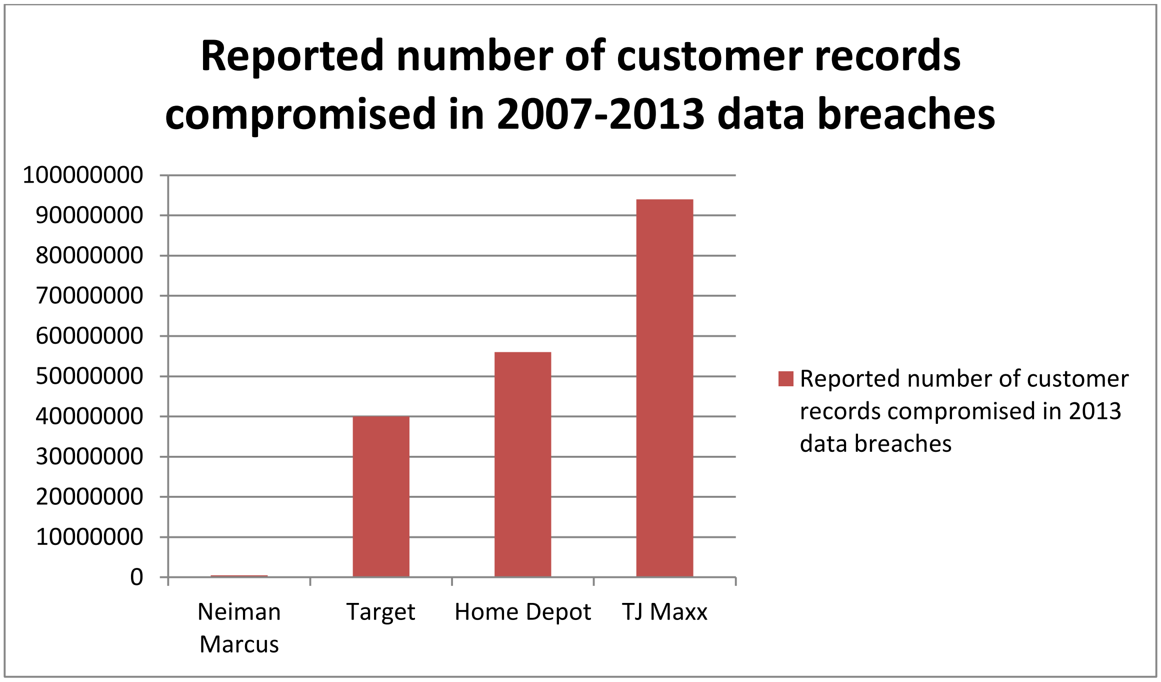
Why every transaction should be tokenized

As tokenization is cheap to implement and can potentially save a company millions of dollars in fraud liability, not to mention save millions of consumers from the headache of dealing with their own compromised credit cards, tokenization seems to be an intuitive choice for *any* business to implement. In many cases, upgrading to a tokenized virtual gateway from a non-tokenized physical card terminal provides ancillary benefits to businesses like better reporting tools and searching features, further bolstering the case for upgrading. Tokenization will be an even more powerful player in the data security world in the years to come; as physical credit card terminal technology has reached its ceiling (and indeed has not changed substantially since its advent in the 1970s), it seems to be only a matter of time until tokenized gateways become the norm. Thus, it makes more sense to start taking advantage of tokenization technology now because there will undoubtedly come a time when physical terminal technology is relegated to obsolescence.

EBizCharge™

Supplementary graphs

Figure 1



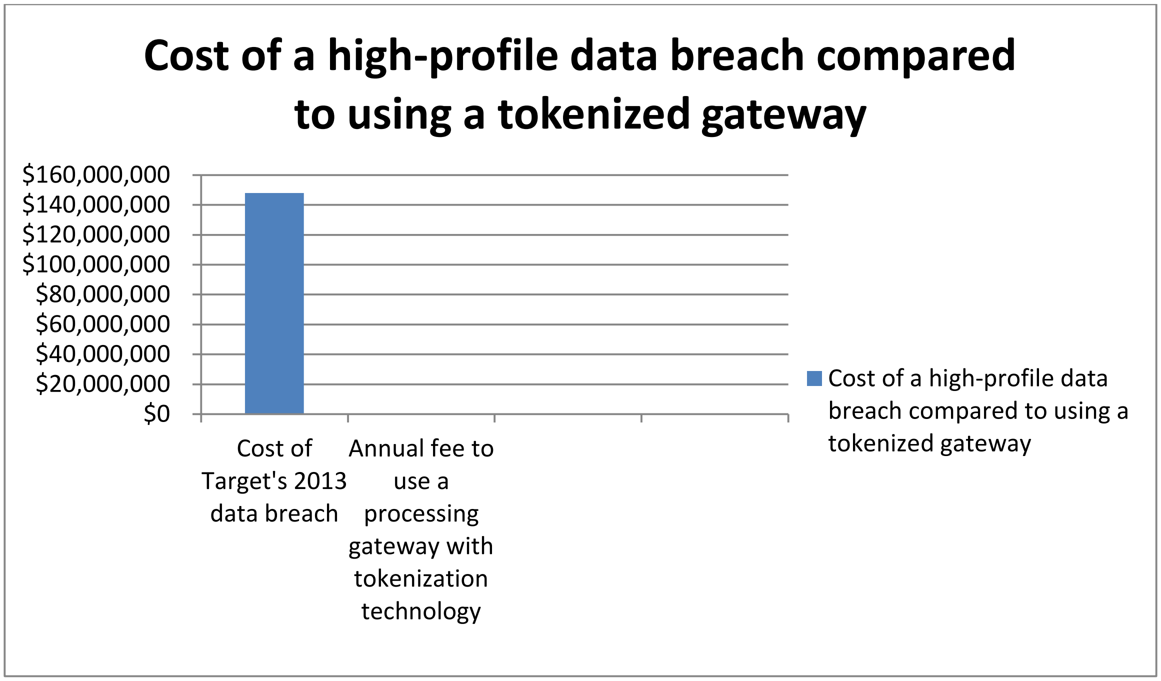
Neiman Marcus: **530,000**

Target: **40,000,000**

Home Depot: **56,000,000**

TJ Maxx: **94,000,000**

Figure 2



Cost of Target’s 2013 data breach: **$148,000,000**

Probable annual cost of using tokenized gateways in all of Target’s 1,683 locations based on $25 flat monthly fee multiplied by 12 months multiplied by 1,683 locations[5]: **$504,900**

Sources Consulted

1. http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data
2. http://www.sctimes.com/story/money/2014/11/25/year-target-data-breach-aftershocks-finally-end/70080462/
3. http://online.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571
4. http://www.nbcnews.com/id/21454847/ns/technology_and_science-security/t/tjx-breach-could-top-million-accounts/#.VHTh1fnF-pw
5. http://pressroom.target.com/news/fastfacts
6. http://philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2010/D-2010-January-Heartland-Payment-Systems.pdf

All citations are from these pages as they appeared November 25th, 2014.