eCommerce in the Wake of Data Theft:

A Three-Pronged Approach to Rebuilding Customer Trust

vantiv®

CNPCardNotPresent.com®

THE INDEPENDENT SOURCE FOR ORIGINAL CNP NEWS

For those who do business in the card-not-present space, 2013 was a tough year on the holiday party scene. Things would start out pleasantly enough, but at some point, inevitably, someone would ask what they do. That meant, inevitably, the subject of the recent, major consumer data breaches would come up. And, inevitably, someone would relate their personal story of a stolen credit card number, introducing a palpable sense of dread to a formerly merry gathering.

> *It's not just the companies that were victims of the data breach that are impacted. Everyone in the ecosystem, everyone in the payment space, everyone in commerce is, in fact, impacted.*

Consumers whose data has been hacked often feel helpless, fearful of what might happen now that their personal data is "out there," and irritated at the inconvenience of having to update all their recurring accounts with reissued card information. According to Nick Stice, vice president of engineering for online marketing company Orange Soda, "I was discussing the recent data breach with a partner, and he felt a sense of relief to know that we were doing everything possible to protect our customers' credit card information, and that we took data security very seriously."

Unfortunately, these hacks are becoming increasingly frequent. According to a New York Times article, "There are now only two types of companies left in the United States: those that have been hacked and those that don't know they have been hacked."[1] The numbers tell the story: The Open Security Foundation reports that in 2012, there were 1,502 documented incidents of loss, theft, and exposure of personally identifiable information—a 40 percent increase from 2011.[2] What's worse, more than 50 percent of data breaches go unreported,[3] because companies are desperate to protect their brand. Lag times between breach and discovery give thieves a big head start: 78 percent of data breaches take weeks, months, or even years to be discovered.[4]

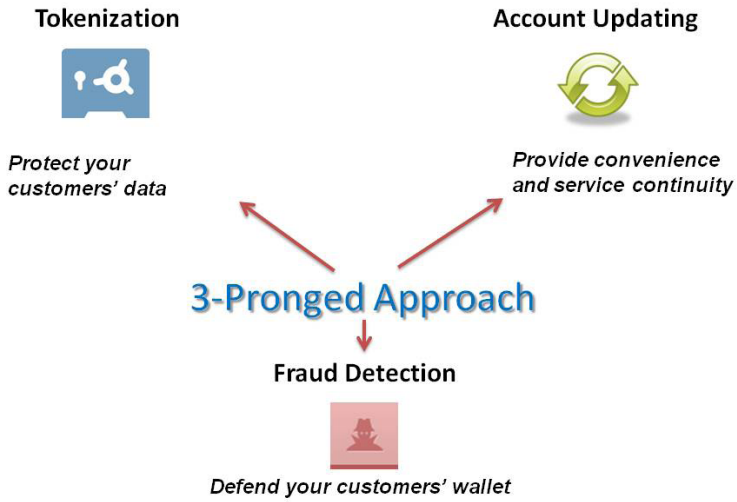
Moreover, the damage goes beyond just the businesses that get hacked. Bill Cohn, director of product management at Vantiv, notes, "It's not just the companies that were victims of the data breach that are impacted. Everyone in the ecosystem, everyone in the payment space, everyone in commerce is, in fact, impacted."

So what can each merchant within the commerce ecosystem do to regain customers' trust? Cohn suggests a three-pronged approach: tokenization, fraud detection, and account updating.

1. Perlroth, N. (2013). The Year in Hacking, by the Numbers. Retrieved from: http://nyti.ms/1h6y8n5.
2. The Open Security Foundation, as reported in IBM X-Force 2012 Trend and Risk Report, March 2013, p.10
3. http://www.digitus-biometrics.com/blog/data-security-breaches-often-unreported-notes-industry-report/
4. 2013 Data Breach Investigative Report; Verizon, p.11

Tokenization

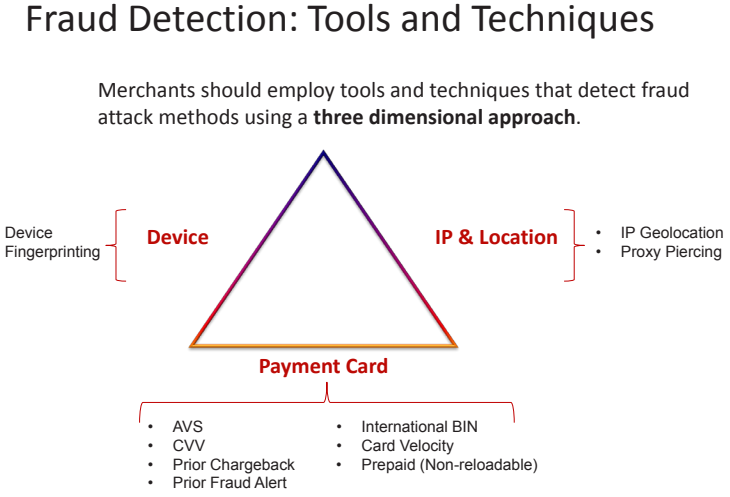
First, merchants can regain customer trust by protecting customer data through tokenization. A token is a benign, untranslatable numerical reference sequence that is useless and worthless outside of the transaction between a merchant and its processor. Using ecommerce data security solutions such as PayPage, Javascript code is placed on the merchant's payment page which on submission replaces the sensitive card data with a non-sensitive value (token) prior to submitting it to the merchant's ecommerce engine. Simply put, thieves can't steal what a merchant doesn't have. Thus, even in the event of a breach, tokenization protects customer data and reduces merchants' exposure.



Of course, merchants have to do more than just protect customer data. They must also take steps to prevent fraudsters from using stolen card numbers to purchase their goods and services. The second prong, therefore, is fraud detection.

Fraud Detection

The link between data theft and fraud is clear: Breaches supply the card inventories that fraudsters demand. There is an increasingly sophisticated black market for selling stolen cards, and it is easier than ever for fraudsters to obtain consumers' personal data. Through fraud detection, merchants can defend their customers' wallets, while protecting themselves from further financial losses due to chargebacks. What's more, fraud detection can help merchants protect their reputation and retain their customers. According to the LexisNexis 2010 True Cost of Fraud Study, more than 36 percent of consumers who are fraud victims avoid certain merchants, and 27 percent say they will spend less money with those merchants.(5)



5. LexisNexis 2010 True Cost of Fraud Study, p.11

Some merchants, particularly smaller businesses, may be tempted to forgo implementing fraud-detection measures, figuring fraudsters won't bother with their site. They would do well to consider, however, that fraudsters are looking to exploit any weakness they can find in the payment system as a whole. They will often use unprotected sites to test stolen card numbers. Once the card gets approved there, they then go and use it elsewhere. "You can't say that detection of fraud is going to regain the trust of the entire ecosystem," says Cohn, "but [you] don't want to be that weak link in the payments chain."

There are a variety of tools and techniques merchants can use to detect fraud, and Cohn believes the most effective systems take a three-dimensional approach, covering (1) the device, (2) the location, and (3) the payment card. Merchants can use device fingerprinting, IP geolocation, and proxy piercing, and then a host of techniques relating to the card itself, ranging from the basic tools (address verification, CVV) to the more advanced (prior chargeback, prior fraud alert, international BIN, and card velocity).

An effective fraud strategy might, for example, fingerprint the device from which a transaction originates and check the velocity on it, that is, check how many times this device has done a transaction in a given period of time. Or, it might check how many times over a given period of time a transaction has been originated from a certain IP address. Filtering transactions through these three dimensions can reveal aberrant behavior patterns that can indicate fraud. Each merchant needs to figure out a strategy that works for their business, bearing in mind that strategies need to be constantly evolving as fraudsters change tactics.

Account Updating

The third prong in the three-pronged approach to restoring customer trust is account updating. When a breach occurs and a customer's card is reissued, the inconvenience of contacting service providers with new card information can be overwhelming and irritating. If a customer forgets to update his card information with a merchant, his recurring payment may not go through and his service or purchase might be delayed or canceled, causing disruption and headaches for himself and the merchant.

According to data accumulated by Vantiv, in the first five weeks of 2014, the overall 'Account Number Changed' account updating response percentage increased about 1.75 times from December 27, 2013 to January 31, 2014. The number jumped from 0.8% to 2.2% in just five weeks' time. Cohn notes, "The issuers have replaced millions of cards, and you, the merchant, can help your customers when these events take place."

Merchants can serve their customers by requesting account updates and applying them on their behalf. This supports continuity of service for the customer and can boost the merchants' revenue by ensuring that payments are collected on time and that the customer's business is retained.

The basic account updating model entails the merchant compiling an account update request file, which they submit to their processor, who submits it to the card networks. They match the accounts submitted with their new account number and send them back to the merchant, who updates the cards on file for the next billing cycle. An advanced account updating service shifts the work from the merchant to the processor: The processor determines which cards to submit to the card networks for an update, then stores the updates locally within their own system. The next time the merchant charges the original account number, the processor automatically substitutes the reissued card number before submitting it to the card networks for authorization.

The issuers have replaced millions of cards, and you, the merchant, can help your customers when these events take place.

Either of these options is preferable to attempting to contact customers directly and asking them to update their information. Nick Stice at OrangeSoda says their company "found that about two percent of our revenue last year was attributed to updated credit card information from subscribing to the account updater service [provided by Vantiv]. That may sound like a small number, but it's actually quite large."

Conclusion

In order for the commerce ecosystem to thrive, it is important for every merchant to do their part to regain and preserve customers' trust. The three-pronged approach of tokenization, fraud detection, and account updating is a way for merchants to regain the customer trust that has been shaken by recent data breaches. Says Cohn, "By demonstrating to customers that you're protecting them, that you're making their lives easier, you can regain their trust and hopefully have a committed, long-term, loyal relationship with them."

About Vantiv, Inc.

Vantiv, Inc. (NYSE: VNTV) is a leading, integrated payment processor differentiated by a single, proprietary technology platform. Vantiv offers a comprehensive suite of traditional and innovative payment processing and technology solutions to merchants and financial institutions of all sizes in the U.S., enabling them to address their payment processing needs through a single provider. We build strong relationships with our customers, helping them become more efficient, more secure, and more successful. Vantiv is the third largest merchant acquirer and the largest PIN debit acquirer based on number of transactions in the U.S. The company's growth strategy includes expanding further into high-growth payment segments, such as ecommerce, payment facilitation (PayFacTM), mobile, prepaid, and information solutions, and attractive industry verticals, such as petroleum, business-to-business, government, healthcare, gaming, and education. For more information, visit www.vantiv.com.

About CardNotPresent.com

CardNotPresent.com is an independent voice generating original news, information, education and inspiration for and about the companies and people operating in the card-not-present space—one of the only sources of content focused solely on this growing segment of the payments industry. Our only product is information. Our only goal is to provide it in an unbiased manner to our subscribers. The company's media platforms include the CardNotPresent.com portal, the hub for news, information and analysis about the payments issues that most affect merchants operating in the space; the CNP Report, an e-newsletter delivering that focused information directly to your email inbox twice a week with no extraneous clutter; the CNP Expo, an annual gathering of the leading companies in the space from the smallest e-commerce Websites and technology providers to global retailers and payment processors; and the CNP Awards, an annual event honoring the products and solutions CNP merchants rely on most to increase sales. For more information, visit www.CardNotPresent.com.