THREE SHORT STEPS - ONE GIANT LEAP FOR ONLINE MERCHANTS

To: ALL Merchants and ISO/MSP's

From: Network Merchants, Inc. (NMI)

Re: Processing Online Transactions

As you know, there are inherent risks associated with handling credit card data. To avoid liability, we strongly recommend you do not process cardholder data, don't transmit it, and don't store it!

For many merchants, this advice seems implausible. Merchants ask, **"How can we process online transactions without handling cardholder data?"** The solution lies within NMI's **"Three Step Redirect™" API**, which is described in this memorandum.

Contents

Network Merchants, Inc. (NMI) is changing the way online merchants process their customer's sensitive credit card data. It's called the **"Three Step Redirect™"** and it's a patent pending interface that provides a secure way for merchants to process transactions through their website without ever touching their customer's sensitive data.

THE PROBLEM – MERCHANT BREACH

Every day, merchants deal with the ongoing threat of thieves breaching their servers or having to discover their customer's personal data has been compromised. According to the U.S. Bureau of Justice Statistics[1], in just one year 7,818 businesses reported data breaches.

- 67% detected at least one cyber attack in which their computer system was the target.
- The majority of victimized businesses (86%) detected multiple incidents, with half of these (43%) detecting ten or more incidents during the year.
- Approximately 68% of the victims sustained monetary loss of $10,000 or more.

WHO'S AFFECTED?

In the United States, fraud crimes affect consumers and the business community in multiple ways. The impact of these crimes clearly touches the parties involved in a transaction at all levels and from many directions. Included below are some of the victims and the ways they are affected.

Merchants

- Experts estimate merchant costs vary from $90 to $305 per customer record[2].
- If breached, or suspected of breach, Merchants pay the cost of PCI-DSS forensic security audit.
- Costs associated with downtime as a result of breach.
- Breach notification requirements including call centers and mail notification.
- Chargebacks, non-compliance fines and penalties.
- Loss of business, tarnished brand and reputation.
- Cost to provide credit monitoring for victims.
- Lost employee productivity.
- Public relations damage control.
- Unable to accept credit cards in the future – "Match List".
- Litigation – witness, discovery, response, and court costs.
- Legal counsel.

Acquirers – ISO's and MSP's

Acquirers, Independent Sales Organizations (ISO's) and Merchant Service Providers (MSP's) are the companies that enable merchants to accept credit cards. These companies understand they have a

[1] http://bjs.ojp.usdoj.gov/index.cfm?ty=tp&tid=41
[2] http://www.forrester.com/rb/Research/calculating_cost_of_security_breach/q/id/42082/t/2

lot to worry about in the event their merchant's data is compromised. When a breach occurs, Acquirers, ISO's and MSP's try to collect non-compliance fines and penalties directly from the merchant. If there is not enough money in the merchant's account, the Acquirers, ISO's and MSP's are ultimately responsible.

According to the U.S. National Archives & Records Administration[3], 50% of all merchants that lost critical data for ten days or more filed bankruptcy. Based on the rate of bankruptcy filings, as well as the realization that most merchants fail to provide notice when a breach occurs, the costs and exposure to liability that Acquirers, ISO's and MSP's face is substantial.

Issuing Banks

The issuing banks are the member banks that issue credit cards to consumers. In most cases, it's the issuing bank that files lawsuits to recoup losses in the aftermath of a data breach. Some of their losses include the cost of reissuing new credit cards, cost of notification and the cost of fraudulent charges.

Cardholders

Victims are often confused. Their ability to trust has been severely tested. They don't know if other personal information was stolen. They're not sure if thieves will use their sensitive personal information at a later date or will distribute personal information to other unscrupulous individuals. According to the Identity Theft Resource Center [4]– 69% of those surveyed said they would stop using a site where their personal information was stolen.

An additional concern cardholders have when their personal information is compromised is identify theft. According to a 2009 study conducted by the Javelin Strategy and Research Center[5], identify theft is on the rise affecting almost ten million victims in 2008. Cardholders are also frustrated with time-loss and hassles involved with securing a new card.

THE DILEMMA – THE CURRENT STATE OF THE INDUSTRY

In an attempt to reduce the number of data breaches in the payment industry, the Payment Card Industry (PCI) Data Security Standard (DSS) was established to provide guidance for merchants to follow and mirror best security practices. PCI security standards are technical in nature and are used to protect cardholder data. The DSS applies globally to all entities that store, process and/or transmit cardholder data. Merchants who accept or process payment cards must comply with the PCI-DSS.

[3] http://www.archives.gov/

[4] http://www.idtheftcenter.org/workplace_facts.html

[5] http://www.javelinstrategy.com/

Even if merchants follow current PCI-DSS requirements, fraudsters have devised ways to hack servers through a variety of techniques. These techniques include spyware, adware, sniffers, phishing, spoofing, port scanning, Trojan horses, malware, viruses and numerous other ways to breach merchant severs and compromise their data. Large merchants spend thousands, if not millions of dollars each year to fight cyber criminals. Small and midsize merchants believe they're immune because the media only reports on large merchant breaches such as TD-Ameritrade, BlueCross Blue Shield, Health Net, Heartland Payment Systems, Sprint, and TJX.

Unfortunately, the small and midsize merchants couldn't be more mistaken. According to Jennifer Fischer, Visa's Director of Enterprise Risk and Compliance, Visa continues to see small merchants most frequently targeted by hackers. The reason for this is fraudsters know large businesses have the resources to protect their data and small merchants do not.

THE SOLUTION

NMI's "Three Step Redirect™" allows merchants to complete online transactions without ever touching the customer's sensitive data.

HOW IT WORKS – EXAMPLE

Catherine, the customer, enters Wally's Website, to purchase his famous Wallpaper. Catherine picks out her favorite design and goes to Wally's 'Check-Out' to make the purchase.

Wally itemizes the products in Catherine's shopping cart and creates an invoice which he sends to the Payment Gateway. The Payment Gateway receives Wally's invoice and responds to Wally, providing him a URL where Catherine goes to enter her sensitive payment information.

Catherine leaves Wally's website seamlessly, and submits her payment information to the Payment Gateway bypassing Wally completely.

The Payment Gateway combines information from Wally's invoice with Catherine's sensitive payment information and returns Catherine back to Wally's Website.

Wally see's Catherine has returned and receives a Token from the Payment Gateway confirming terms of the transaction. Wally can then continue to suggest other items for Catherine to purchase, or instruct the gateway to process the transaction.

Important points to consider relative to the above transaction:

1. Wally, the Merchant, never touched Catherine's sensitive payment information. As a result, Wally drastically increased his company's security, decreased his liability, all while minimizing the cost and complexity of industry regulations and standards; especially the Payment Card Industry Data Security Standard (PCI-DSS).

   ✓ Note: Tokenization exchanges sensitive payment data, such as the credit card's account number and expiration date with unique identifier symbols. Through a direct encrypted SSL connection, Catherine's computer transmits sensitive payment information to the Payment Gateway's secure servers instead of through Wally's potentially insecure environment.

2. Catherine, the Customer, never knew she left Wally's website. The look and feel of the entire transaction remained seamless. Wally was able to maintain his own look and feel throughout.

   ✓ Note: Instead of the Payment Gateway dominating the payment portion of the transaction, Wally's website encapsulates the Payment Gateway and remains in the forefront of his customer's experience throughout the entire transaction.

3. The Payment Gateway and Wally were always in sync. Wally knew exactly when the payment was authorized and he controlled the transaction from start to finish. He knew when Catherine returned to his website and when the transaction was processed. Wally didn't experience typical payment gateway errors, such as not knowing a payment was made when a customer prematurely exits the gateway. Wally shipped the product with full knowledge the transaction was paid.

   ✓ Note: It's common with current redirect methodologies that Customers can leave the Payment Gateway after the payment has been processed but before returning to the Merchant's website. In that event, the Merchant lacks knowledge on the status of the transaction. It happens often, computers crash, internet connections fail, customers accidentally close their browsers, etc. In all those cases, the customer's card may be charged but the merchant doesn't know to ship the product. These scenarios likely result in chargebacks.

4. When Catherine returned to Wally's website, after submitting her sensitive payment information, Wally was free to up-sell her other products like paper, trays, glue and brushes, or; he completes the transaction in its current state.

   ✓ Note: Current redirect methodologies don't allow Merchants to up-sell their Customers. Conversely, the Three Step Redirect™ API allows merchants greater flexibility and increased sales even after the customer payment information has been collected.

CONCLUSION

Traditionally, payment gateways provide a one-dimensional transaction transmission process where sensitive payment information is transmitted and stored in the merchant's environment. Customer information from the merchant's website can be compromised by fraudsters through a variety of methods.

NMI’s Three Step Redirect™ is a methodology where sensitive credit card information is transmitted directly to the payment gateway through an end-to-end Secure Sockets Layer (SSL) connection, bypassing the merchant's server and payment application. The solution ensures secure data transmission by keeping merchants from seeing, touching, handling, transmitting, or storing any sensitive payment details. And since it takes merchants outside the scope of handling sensitive payment information, it minimizes the cost and complexity of industry regulations and standards; especially the Payment Card Industry Data Security Standard (PCI-DSS).

For over a decade, NMI engineers have been designing technology that delivers industry leading payment applications. Its patent pending Three Step Redirect™ was a complicated and time consuming challenge, but engineers worked through many iterations until finally discovering a solution that provides the utmost flexibility while simultaneously shielding merchants from potential liability.

The payment industry is going through a tumultuous time. For years, merchants and their developers have been plagued by shortcomings in existing redirect technologies. New and innovative ideas are required to take the industry to the next level and NMI’s Three Step has done just that.

Contact Information:

For more information regarding NMI’s Three Step Redirect™ API, please contact NMI at (800) 617-4850, or send an email to: info@nmi.com.