

# DATA COMPROMISE BASICS

MERCHANT SECURITY SERIES  
ISSUE #1

---



[WWW.PROPAY.COM](http://WWW.PROPAY.COM)

## Table of Contents

Preface .....	3
I am a small merchant. Why would data thieves target me? .....	3
How do data thieves get my data? .....	4
I am scanning my site as required by the PCI DSS. Doesn't this protect me? .....	7
I have a firewall as required by the PCI DSS. Doesn't this keep hackers out of my computer? .....	7
I am running anti-virus as required by the PCI DSS. Doesn't this protect me? .....	8
How will the card brands know I have been hacked? .....	8
What really happens after a compromise?.....	8
If I am PCI DSS Compliant will I be given safe harbor from fines? .....	9
Won't my cyber-insurance protect my organization? .....	9
What is the answer? .....	9
How can ProPay Help? .....	9
About ProPay .....	11

## **Preface:**

This document is intended to provide an overview of some tactics and technologies used to gain unauthorized access to systems and applications. The intended audience is small merchants with limited networking expertise. For this reason some of the discussions have been generalized and some of the more complex discussions have been intentionally left out. As an example, this document talks about ports without discussing the differences between UDP and TCP ports. We also talk about firewalls without discussing the differences between Layer 3 and Layer 7 devices. This is done intentionally, to provide useful information to those readers that do not have a strong background in information security.

Data security can be a complex subject. It has become increasingly common to read about some merchant that has been the recent victim of a data compromise. Credit card data, social security numbers, bank account numbers and other data are the new targets of criminals. Unfortunately, many small merchants mistakenly believe that either they are not targets of criminals due to their size or that their security will prevent a criminal from successfully stealing their data. This paper is intended to provide a brief overview of how hackers can steal data and answer questions commonly asked by small merchants.

## **I am a small merchant. Why would data thieves target me?**

It is a common misperception that data thieves only target large, well known organizations. In fact, the card brands (Visa, MasterCard, etc.) have frequently stated that over 80% of identified compromises of cardholder data (credit, debit card data) involve Level 4 Merchants. Level 4 Merchants include small restaurants, ecommerce merchants, and even independent sales consultants of direct selling companies. While larger, more well-known companies often make the front page of newspapers, there are dozens of smaller companies that are victimized for every large or well-known company that suffers a data compromise.

It is important to understand that companies are typically not targeted because of their size or brand. More often they are targeted simply because they provide an easy opportunity for data thieves to quickly steal data. Smaller companies don't usually have the resources available to protect their assets that larger companies do and smaller merchants often have significant amounts of data.

Consider a more common example of home burglaries. Burglars don't typically break into banks or mansions even though they would likely be able to steal more money or more valuable items. Burglars typically break into normal houses and offices. Why? They present an easier opportunity with less risk than the larger organization. There are, of course, burglars that specialize in mansions and bank vaults, but these represent a small percentage of actual thefts.

## How do data thieves get my data?

While scores of books are written on this particular topic, this paper will attempt to provide some basic insight into common methods that criminals use to compromise small merchants. In general hackers can actively attempt to break into systems or they can passively wait for the merchants to do the work for the hackers. First, let's discuss some of the active techniques. This paper will discuss some of the more basic steps involved.

Identification of targets: Many people mistakenly believe that because they do not have a website or that they are a small company that they are hidden from hackers. This is similar to the "out of sight, out of mind" mentality. Such an assumption is a huge miscalculation that has resulted in numerous small merchants being victimized. It is important to understand that every computer (server, laptop, desktop etc.) that has Internet access has what is known as a 'routable' or 'public' Internet Protocol (IP) address assigned to the system, or a system on the network (firewall or router). Without such an address people could not access their favorite websites, send email, or chat. While Internet users are all accustomed to typing in the domain name ([www.domainname.com](http://www.domainname.com) for example) of the site they wish to visit, every domain name is also associated with an IP address. As an example, you can reach [www.cnn.com](http://www.cnn.com) by either typing the domain name or the IP address of 157.166.255.19 in your browser bar. The domain names are resolved through a service known as Domain Name Service or simply DNS. For companies with a registered domain name, finding the system that resides behind the domain name is as easy as using ping or a basic "whois" lookup. You can try this on a number of sites including: [www.selfseo.com](http://www.selfseo.com).

To identify the IP that you are currently using, you can visit [www.whatismyip.com](http://www.whatismyip.com). This will show the current IP address assigned to your computer or network edge device (firewall or router). If you have a public IP address (which you do or you would not be able to access the Internet) then your IP is visible to the entire Internet.

So now you are likely wondering how a particular criminal may know where your system is located if you don't have a registered domain name. To have Internet service you signed up with an Internet Service Provider (ISP) such as ATT or Comcast. These ISPs have ranges of registered IP addresses that they, in turn, provide to their own clients. If a criminal can find a particular IP range of a service provider they can scan the range using common tools and identify active systems associated with the IP addresses. For example ATT 'owns' the IP range 12.0.0.0 – 12.255.255.255. While this is a very large range of IP addresses, a criminal can scan any of the IPs in the 12.x.x.x range and potentially locate a system. Many systems (firewalls, computers, routers) are configured to respond to what is known as Ping request. **Ping** is a computer network administration utility used to test whether a particular host is reachable across an Internet Protocol (IP) network and to measure the round-trip time for packets sent from the local host to a destination computer, including the local host's own interfaces. If a system responds to a ping request, the attacker knows it is a 'live system'. Once a live system has been identified, then it is a matter of identifying the potential ways to exploit the system.

Ports, Ports and more Ports: Once a criminal has identified a particular IP address of a system that they wish to target, the next step is to attempt to quickly understand the type of programs or services the system may be running. A port is an application or service-specific construct serving as a communication endpoint. Every computer has 65,535 ports available. Some ports are registered to common services such as Hypertext Transfer Protocol (HTTP-port 80), Secure Hypertext Transfer Protocol (HTTPS) (port 443), and Simple Mail Transport Protocol (SMTP-port 25). Even some games have registered ports. Doom for example uses port 666 to allow gamers to coordinate and play games online. Identifying the ports, and the likely services running, is easily accomplished by conducting a basic port scan of the IP address. If you visit an Internet website, the website is being accessed by your computer over port 80. If you send email you are using port 25. By scanning a particular IP address and identifying “open ports” criminals can make educated guesses or assumptions as to what type of system is associated with the IP address. For example, if a port scan reveals that port 80 and port 443 are ‘open’ and responding, the hacker knows that the system is allowing HTTP and HTTPS inbound. This strongly suggests that the system is running a web server. Since port 443 is used for securing (among other things) ecommerce transactions, it suggests that the system may be accepting ecommerce data. If port 1433 is identified, this suggests that the system is running a SQL Server (database), as SQL Server communicates over port 1433. By understanding what types of systems are running, the criminals have more information on which to target the organization.

Now that we have very basic understanding of ports and IP addresses, we can move on to other topics.

Websites: While it is possible to gain a lot of information from scanning IP addresses, if a company has a website then they have already provided a significant amount of information to the data thief or hacker. If a hacker visits your website and sees that you accept credit card transactions, they know that 1) you likely have valuable data entering your website and 2) there are opportunities to access the system. Often we like to think that hackers are using sophisticated technologies to conduct reconnaissance when it often only requires a simple visit to a company’s website. In fact, some of the most common forms of reconnaissance involve simple website visits and a review of the technology used. Understanding the type of website and the brand of ecommerce shopping cart being used can provide a significant amount of data to a criminal.

Vulnerability Identification: Once the IP addresses and ports are identified, the hacker then will identify what, if any, vulnerabilities exist in the system or application. Anyone who has a computer is familiar with installing patches and upgrades. These patches are intended to fix specific vulnerabilities that have been identified. The Common Vulnerabilities and Exposure (CVE) is a dictionary of common names of vulnerabilities. To date, CVE lists over 42,000 vulnerabilities. You can read more about CVE at <http://cve.mitre.org> to identify whether a site is vulnerable to a particular exploit, hackers will use common tools such as Nessus’ ([www.nessus.org](http://www.nessus.org)) vulnerability scanning tool. A Nessus scan will identify whether the system has any number of vulnerabilities which may be able to be exploited. Once a vulnerability is identified, the hacker can use an exploit to take advantage of the vulnerability. Sometimes the vulnerabilities are somewhat benign and other times they present a very serious security issue for the merchant.

In addition to system level vulnerabilities, websites may also have application layer vulnerabilities present. These are much more difficult to detect and fix than system or network layer vulnerabilities.

As discussed in the previous section, sometimes a simple visit to the website and a basic Internet search will reveal a number of vulnerabilities. As an example (and not to pick on one technology) a very common open source eCommerce shopping cart is OS Commerce. On November 19<sup>th</sup>, a serious vulnerability was identified that allowed an attacker to bypass the authentication and access the administrative pages. If an attacker could identify that you were using OSCommerce, they would know immediately that you were likely vulnerable to this particular exploit.

SQL Injection: One of the most dangerous and commonly exploited vulnerabilities is known as SQL Injection. SQL is short for Structured Query Language and is the language used for managing data in structured database systems. SQL Injection is a type of attack that inserts unexpected strings of code into websites fields. The website application in turn passes these commands to the database which responds accordingly. SQL Injection attacks can be used to retrieve usernames and passwords directly from a web application or can be used to extract credit card data directly from a database. Traditional firewalls (layer 2, 3, 4) cannot protect against SQL Injection attacks because they exploit vulnerabilities at the application layer (layer 7). It is estimated that over 90% of websites are vulnerable to SQL Injection vulnerabilities.

Passive Methods: It is widely believed that companies that are compromised have been hacked by some criminal genius that has managed to circumvent the company's security controls. Sadly, the hackers are often unintentionally invited into the systems by the company's own employees. Data thieves often employ compromised websites that infect visiting computers. These are known as 'drive by' infections and require no effort on the part of the hacker. McAfee recently identified the search term "Jessica Biel Screensaver" as its most dangerous search term on the Internet. If a person queries the term on a major search engine almost one half of the websites that are returned will download malicious software onto the user's computer if accessed.

Other popular methods of infecting systems include sending infected emails to individuals and pre-infecting thumb drives and other media in the hope that someone will insert into their computers. Although we like to think that our employees would not open such emails or use thumb drives found in the parking lot, statistics demonstrate that often employees will in fact do so.

Malicious Software: While the methods described so far discuss how the criminals identify and gain access to systems, their objective in gaining that access is to steal valuable data. This is where malicious software comes into play. Malicious software is a broad category of software that includes viruses, worms, Trojans, adware, spyware, and other types of software that are designed with malicious intent. As Verizon stated in their 2009 Data Breach Report; "Hacking gets the criminal in the door but malicious software gets him the data." Criminals will use a variety of methods to get access to the systems in order to install malicious software. Two of the more common forms of malicious software used to steal credit card data include Trojan Sniffers and Screen Capture Trojans.

Trojans are applications that are designed to look like other benign applications. Because they are not recognized as malicious they can operate without detection. Sniffers are a type of application that are designed to 'sniff' network or computer traffic and copy the traffic to send to a third party. Credit card data is often the target of Trojan sniffers. Screen capture programs are used to capture sensitive data such as credit card or bank account data as it is entered into websites or to capture login information that can then be used to login to the systems directly.

Once installed, malicious software can be extremely difficult to detect and remove.

### **I am scanning my site as required by the PCI DSS. Doesn't this protect me?**

The Payment Card Industry Data Security Standard is a set of 12 high-level requirements designed to protect payment card data from compromise. Merchants are required to comply with the PCI DSS at all times.

PCI DSS requirement 11.2 does require that Internet facing IP addresses (see the previous section) be scanned by an Approved Scanning Vendor (ASV). This does not guarantee that you are protected against hackers. There are currently over 41,000 identified vulnerabilities with only about 3,500 that are detectable by Nessus. The ASV scanning program identifies about 300 of these vulnerabilities. This only accounts for about 10% of the total that Nessus includes in their file. In addition, new vulnerabilities are identified on a daily basis. New exploits that take advantage of vulnerabilities for which patches or other fixes have not yet been developed are known in the security industry as zero-day exploits. Scanning cannot detect zero-day exploits as they have not yet been identified.

Consider a situation in which you have a quarterly PCI scan on January 1<sup>st</sup>. On January 2<sup>nd</sup> an exploit is identified and the scanning vendors begin updating their scanning engines to detect the exploit. Your company's next scan is on April 1<sup>st</sup>. During the time from January 2<sup>nd</sup> through April 1<sup>st</sup>, you are unaware of the vulnerability and once identified you are still required to take corrective action to address the vulnerability. In this scenario, your company could have a serious vulnerability for over 4 months that exposes your company to attack from hackers.

Another example is that of the SQL Injection vulnerability that was discussed earlier. SQL Injection is an application layer exploit that cannot be accurately detected by a PCI scan. It is completely possible to pass a PCI scan and be vulnerable to SQL Injection attacks.

### **I have a firewall as required by the PCI DSS. Doesn't this keep hackers out of my computer?**

Firewalls are required by the PCI DSS and are a very important component of any data security program. It is important to understand how firewalls work and their limitations. A firewall is a device or application that blocks particular traffic based upon certain criteria. For example, a firewall can be configured to block all traffic from a particular IP range. Firewalls however only block certain traffic and allow other traffic.

If you need to send email, for example, the firewall would need to allow SMTP (port 25) traffic outbound or you could not send email. If you have a website and accept ecommerce payments your firewall would need to allow HTTP and HTTPS (port 80 and port 443) inbound otherwise people could not access your website or allow customers to make purchases. Using a properly configured firewall *restricts* the ability of a hacker to access your systems, but it does not completely prevent access. The more access that is allowed into the network, the more opportunities hackers have to identify and exploit vulnerabilities.

### **I am running anti-virus as required by the PCI DSS. Doesn't this protect me?**

Like scanning, anti-virus is an important part of a well designed security program. With that in mind, it is important to understand the limitations of anti-virus applications. Like scanning, malicious software protection can only detect those malicious applications that have first been identified and for which a signature has been defined. For this reason anti-virus and other forms of malicious software protection is reactive. This means that it will only detect malicious software for which it has a signature. Malicious software that has not yet been identified is virtually invisible to the detective methods. A good example of this in practice is that of the Sinowal Trojan. The Sinowal Trojan was undetected from early 2006 through 2008. By the time it was finally detected by RSA researchers over 300,000 bank account logins had been stolen.

To further complicate matters, creating custom designed malicious software that is undetectable by commercial anti-virus and other malicious software protection applications is relatively easy. Programs such as Pinch 2.0 Trojan building tools are easily obtained on the Internet. Remote administration tools (Backdoor programs) such as Turkojan are also easily obtained and very difficult to detect.

### **How will the card brands know I have been hacked?**

In 9 out of 10 cases it is the card brands that identify the compromise before the merchant. This is accomplished through a process called a Common Point of Purchase (CPP) investigation. A CPP is similar to the techniques that are used to track food poisoning in restaurants. In a very basic sense, CPPs use fraud patterns as the basis of their investigation. The card brands track the fraudulent cards' past usage over a period of months and look for common points of purchase in which a percentage of cards were used. It is this common point of purchase that is likely the source of the data compromise. The card brands have become very effective at detecting data compromises and can use as few as 10 fraudulent transactions to track a compromise to a particular merchant.

### **What really happens after a compromise?**

When your company has been identified as a potential point of compromise you will be required to engage a forensics company to evaluate your systems and applications for evidence of compromise.

It should be noted that if your company is contacted by the card brands or banks, they have already identified your organization as a common point of purchase and it is extremely unlikely that a forensics investigation will not confirm their suspicions. If the forensics investigation identifies evidence of a compromise you will then be subject to fines, fees, and other penalties from the card brands.

### **If I am PCI DSS Compliant will I be given safe harbor from fines?**

In theory, if your company meets two specific criteria you may be protected from fines. First, you have to have been validated as fully compliant within the previous 12 months and second, you must be fully compliant at the time that the compromise occurred. While safe harbor is a consideration in theory, in practice it is highly unlikely that your company will be able to demonstrate that you met the two criteria referenced above. Consider the two most relevant examples of PCI DSS validated companies that were compromised; Heartland Payment Systems, and RBS WorldPay. Both of these organizations were validated as fully compliant over several years by well respected Qualified Security Assessors (QSAs) and upon investigation were found to be non-compliant during the time of the breach.

### **Won't my cyber-insurance protect my organization?**

This question is similar to asking why a seatbelt should be worn if the occupants have health insurance. While insurance does provide some risk mitigation it does not cover all of the costs or obligations associated with a data compromise. There are currently 46 state data breach notification laws in the US. Cyber-insurance will not provide complete protection against the potential litigation, brand damage, or fines associated with a data compromise. As with anti-virus and other risk mitigation controls it is a good tool, but only provides limited protection.

### **What is the answer?**

What many payment card security experts have learned over the years (this author included) is that the only real way to mitigate the risk of a data compromise is to simply remove the object of value from the equation. In this case it is to remove the cardholder data and thus remove the target of the data thief's efforts. Consider a bank that has no money. There is little value in a criminal taking a risk to break into or rob such a bank. Even if they do decide to try to rob the bank or break into the vault there is nothing of value to be stolen. It is much the same way with data. As ProPay says: "Remove the data, Remove the risk®"

### **How can ProPay Help?**

ProPay provides a robust, secure End-to-End Payment Security Solution, called ProtectPay®. ProtectPay offers organizations the ability to securely process payments without incurring the risk that is often associated with the transmission and storage of sensitive cardholder data. Clients can reduce or remove their compliance obligations and transfer the risks associated with data compromise.

This allows ProtectPay users to re-focus their attention on enhancing their core business and better service their customers while offloading their data protection issues. The features and benefits of ProtectPay include:

- **Secure Storage of Customer Data** - ProPay has been certified as a PCI DSS compliant Service Provider for more than six years. As an early adopter of the data security standards, ProPay has developed a core competency in the protection of customer data.
- **Alternative Payment Methods** - ProtectPay provides the ability to store multiple payment cards for one customer. Additionally, the ProtectPay solution allows the use of alternative payment methods.
- **Encrypted Data Collection Methods** - ProtectPay encrypts sensitive data from the point of customer entry, whether online or in person, so that the merchant or organization never has to store, transmit or process that data. This is accomplished using our MicroSecure® Card Reader, our Payment Management Interface, Seamless Payment Interface and our Virtual Terminal.
- **Repeat Billing** - ProtectPay allows the data to be stored securely while allowing the merchant to use the data for repeat billing and ongoing business transactions.

These features are designed to allow the merchant to continue transacting business as usual, without the worry of data protection and compliance issues. The service is the natural evolution of ProPay's longstanding mission to provide simple, safe, affordable processing solutions.

## About ProPay

ProPay leads the market in providing simple, safe and affordable credit card processing and electronic payment services for businesses ranging from the small, home-based entrepreneur to multi-billion-dollar corporations and enterprises. Whether you're a small business or a large corporation, ProPay provides simple, safe and affordable merchant services and can help secure your payment data through robust encryption and tokenization. Call us today at (888) 227-9856 or email us at [sales@propay.com](mailto:sales@propay.com).

### Corporate Headquarters:

3400 Ashton Boulevard, Suite 200  
Lehi, UT 84043  
(888) 227-9856

[www.propay.com](http://www.propay.com)  
[sales@propay.com](mailto:sales@propay.com)

© ProPay, Inc. All rights reserved.

*The information contained in this document represents the current view of ProPay, Inc. on the issues discussed herein as of the date of publication. It should not be interpreted as a commitment on the part of ProPay, Inc. and ProPay, Inc. cannot guarantee the accuracy of the information presented after the date of publication. Specifications and content are subject to change without notice. This document is for informational purposes only. PROPAY, INC. MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.*

*ProPay is a trademark of ProPay, Inc. Other product or company names mentioned herein may be the trademarks of their respective owners.*