



From the

# Heartland Newsroom

Insights, articles and news  
[HeartlandPaymentSystems.com](http://HeartlandPaymentSystems.com)

## Your Business's Data Has Been Compromised. Now What?

By Kris Herrin, Chief Security Officer  
Heartland Payment Systems

As a merchant, there are some headaches you should try to avoid — and being compromised is one of them.

In a recent survey of credit card compromises, 54% were within the food services industry, and 25% were within the retail industry.<sup>1</sup> If your business is compromised, private information — stored on items like a laptop, office server or point-of-sale (POS) system — may have been illegally accessed and could lead to credit card data theft, fraud and financial loss. In response to what this can mean to merchants and their customers, the Payment Card Industry Data Security Standard (PCI DSS) has raised data protection standards for businesses. They are now mandatory for every business that processes credit or debit card information — including merchants and third-party service providers that store, process or transmit credit/debit card data. But, even if you take steps to increase data security and follow PCI DSS, you still may be at risk. It's important to know what to do if you're compromised, as well as the steps to prevent it from happening.

### What are the signs you've been compromised?

In some cases, if your business is compromised — by wily hackers or malicious software — you may discover the breach by your POS system behaving oddly or strange files with credit card data suddenly appearing. However, most times your POS system will function as it normally does, and you won't be able to tell that anything is different or wrong. You'll likely find out you've been compromised when you're contacted by an issuing bank, credit card company or law enforcement agency that has traced suspicious credit and debit card activity back to your business.

### What are your next steps if you've been compromised?

Once it's determined that your business has been compromised, it's important to make sure you don't do anything to your POS system in case investigators need to complete a forensic investigation. Investigators may use highly specialized tools to examine your system for evidence to help determine how and when your system was first compromised as well as identify cardholders who have been affected. Follow these steps to ensure an efficient investigation:

1. Stop using the POS system. Don't turn the system off, but do disconnect the phone and internet cables from the wall.
2. Don't make any changes to the system. Don't log on, upgrade any software, add new software programs or change any passwords. By disconnecting your system without turning it off and not making any changes, data on your POS remains the same. You'll avoid destroying any evidence that could help investigators track down the hacker and where and how the compromise occurred.
3. Immediately contact your payments processor. Your IT team, local law enforcement and/or Secret Service can help you as well. Your payments processor will notify the card companies and issuing banks about the breach. The card companies will determine whether or not an independent forensic investigation is required.
4. If an investigation is required, you're responsible for finding a vendor/investigator the card companies have qualified to work on security incidents, also known as a Qualified Incident Response Assessor (QIRA). Visit [Visa.com/cisp](http://Visa.com/cisp) for the most recent list of qualified investigators.

### What can you do to prevent a compromise?

How can data breaches be prevented? Many happen because businesses fail to take steps to protect their business and their customers. For example, a business may be running on POS software that is outdated — software that stores data, hasn't been upgraded, or is one that's known to be vulnerable to data breaches. Businesses that use their POS systems as general computers — for tasks such as surfing the internet or back office duties — also increase the risk of downloading malicious viruses that can compromise the system or make it easier for hackers to access your programs.

Being compromised can also happen if your business is not PCI DSS compliant. To be PCI DSS compliant, ask your POS installer and processor about the system you use and if it is up-to-date. Also, speak to your IT specialist about network and data access security, such as firewalls, remote

<sup>1</sup>Trustwave Global Compromise Statistic available from [trustwave.com](http://trustwave.com)

access and external file transfer. Again, visit [Visa.com/cisp](https://www.visa.com/cisp) for the latest PCI DSS requirements. (See the sidebar “Decrease Your Chances of Being Compromised” for more information.)

Your business’s data — and your customers’ information — are valuable. Be sure to protect yourself and your customers by using only up-to-date POS software and by making sure you’re PCI DSS compliant. Taking these steps can save you and your customers from the headaches that go along with being compromised — possible forensic investigations, damage to your reputation, the loss of loyal customers as well as stiff fines — ranging from tens of thousands to hundreds of thousands of dollars — from credit card companies.



*Kris Herrin, a Certified Information Systems Security Professional (CISSP), is the chief security officer at Heartland Payment Systems and an adjunct professor at the University of Dallas Graduate School of Management. Heartland, a NYSE company trading under the symbol HPY, delivers credit/debit/prepaid card processing, payroll, check management and payment solutions to more than 250,000 business locations nationwide.*

*Heartland is the founding supporter of The Merchant Bill of Rights, a public advocacy initiative that educates merchants about fair credit and debit card processing practices. For more information, contact Heartland Payment Systems at 866.941.1HPS (1477) or visit [HeartlandPaymentSystems.com](https://www.HeartlandPaymentSystems.com) and [MerchantBillOfRights.com](https://www.MerchantBillOfRights.com).*

## Decrease Your Chances of Being Compromised

Here are some guidelines to help you decrease your chances of being compromised:

1. Make sure your specific POS software version meets PCI DSS standards, such as those listed on Visa’s Validated Payment Applications list found at [Visa.com/cisp](https://www.visa.com/cisp). Your payments processor — such as Heartland Payment Systems — can also tell you if your software is on the list of vulnerable systems. If your software is listed on the vulnerable systems list, or isn’t listed on the Validated Payment Applications list, ask your POS installer about upgrading your system to a new version or changing to a different, validated application.
2. Make sure your network in general is PCI DSS compliant. For more information, visit [PCISecurityStandards.org](https://www.pcisecuritystandards.org).
3. Don’t use your POS system as your personal computer — i.e., don’t use it to surf the internet, do your bills, etc. This also applies to your employees who use the POS system when you’re not around.
4. Completely remove all files from your old POS software. You may have done the right thing by upgrading your system to a validated one, but simply uninstalling the old program doesn’t always remove all the files — or customer data and card information — from the hard drive, so talk to an IT person to make sure this is actually done.