globalpayments

DATA SECURITY UPDATE

A Merchant's Guide - What to Do if You're Compromised

"The cost of a forensics investigation starts at around £2,500 and can easily cost as much as £10,000 or more."

What's a Data Compromise?

A data compromise or a data breach is a breach of security leading to the accidental or unlawful disclosure of data that you process for your customers, which criminals could use to commit fraud. The information of most value to criminals includes your customers' card numbers, card expiry dates, names, addresses and card security details, such as CVC and track data.

Your business could be a target for criminals, so don't fall into the trap of "It won't happen to me". The costs for investigating and remediating a breach can be very high along with stress, anxiety and the possible disruption to your business.

If you suffer a data breach, you may be required to conduct a forensics investigation to determine the cause of the breach and may be required to re-attest your Payment Card Industry Data Security Standard (PCI DSS) compliance. The cost of a forensics investigation starts at around £2,500 and can easily cost more than £10,000. There are also other costs associated with a data breach post event, including Card Schemes penalties and the costs for achieving and maintaining PCI DSS compliance. These fees can be of similar size but can easily be much more.

It doesn't stop there as there's the possibility that your business may incur adverse publicity, which can lead to the loss of your customers' trust in your brand.

How Does a Data Compromise Occur?

If the breach is deliberate and unlawful, criminals could gain access to your customers' information in many ways, including:

- Hacking your website or computer network and Point Of Sale equipment;
- Through your Third Party Merchant Agents or Payment Service Providers (PSP), such as your web hosting company, who may have not taken the necessary precautions to safeguard your customers' data that you've outsourced to them;
- A dishonest member of staff accessing and passing on cardholder information to criminals; or
- Theft of terminals and terminal receipts from premises.

How Do I Know if I've Been Compromised?

Merchants become aware of a breach in many ways, including system generated incident alerts, unexpected changes to their web pages or files on their website, or from alerts through their PSP. Most merchants only find out through their customers or from their acquirers once fraud starts to occur on the compromised card data. The damage has

already been done by this time. However, you can take remedial action as soon as you find out to limit further damage and costs.

How Can I Reduce the Risk of a Compromise?

Ensure that not only your business is PCI DSS compliant but also all the PSPs that process your payment data are too.

Follow these best practices to protect card data:

- Use strong passwords;
- Don't write down passwords and don't use vendor supplied default passwords;
- Use firewalls and up to date anti-virus software;
- Install the latest patches that are published or supplied by your vendors;
- Check all equipment such as payment terminals for tampering;
- Restrict or limit access to the systems internally;
- Be vigilant to phishing attacks; and
- Perform regular scans for vulnerabilities.

I Think I've Been Compromised - What Should I Do?

If you suspect that your business has suffered a data breach, there are immediate steps you can take to minimise the possible damage and achieve compliance quickly.

If you notice any unusual activity or suspect that your business has been compromised, we strongly recommend taking the following action:

1. Contact Global Payments on 0345 702 3344* immediately and report the incident;
2. Contact your data security incident management team and follow your incident response plan;
3. Notify the local law enforcement agency.

To minimise further data loss, preserve evidence and facilitate the investigation process, follow these 'Dos' and 'Don'ts':

- Don't access, alter or delete files in the compromised system(s).
- Don't attempt to change passwords on the compromised systems.
- Don't log in as ROOT.
- Don't turn off the compromised system(s).
- Do isolate the compromised system from the network (i.e. unplug network cable).

If access to the compromised system can't be avoided, then keep detailed records of what action(s) have been taken with the dates and time, and:

- Do preserve logs (for example, security events, web, database, firewall etc.).
- Do change the Service Set Identifier (SSID) (if using a wireless network) on the wireless access point (WAP) and other systems that use WAP (with the exception of any systems believed to be compromised).

Monitor traffic on all systems that contain cardholder data. Be on 'high alert' and ensure you log all actions taken. By self-reporting any suspected breach early, you can help to reduce the impact to your business.

If in doubt, contact Global Payments immediately on 0345 702 3344*, selecting the option for 'all other enquiries' and report any incidents. We'll support you fully whilst you address the breach and ensure you can continue taking card payments.

*Lines are open Monday to Friday, 9am – 6pm, excluding public holidays. To help us continually improve our service and in the interests of security, we may monitor and/or record your telephone calls with us. Any recording remains our sold property. We also provide a Textphone service on 0345 602 4818.