Data Breach Response

A Nine-Step Guide for Smaller Merchants

Data breaches at large retailers draw plenty of media attention. But, by far, the most common targets of data breaches are not big businesses. They are small merchants.

That being the case, no matter the size of your business, it is important to have a data-breach response plan in place. In fact, PCI standards now require it.

Whether you are sitting down to prepare such a plan or have found yourself the unfortunate victim of a data breach, the following nine steps are designed to help guide you through what can be unfamiliar territory. The most important thing to remember is that prompt action is key. The risks associated with a data breach do not go away when a data breach is ignored; they grow-exponentially.

1. Don't Cut Power! Your first instinct upon learning that you may have been the victim of a data breach may be to "pull the plug," i.e., power down your payment network and devices or log into those systems to alter passwords and security settings. While it is important to act quickly to stop a breach that may be in progress, you should act with care to preserve evidence, insofar as possible, of how your system may have been compromised. Although you should consider isolating compromised systems from your network (e.g., by unplugging network cables, not power), powering down the system or altering log-in information can destroy critical data that may prove helpful as the data breach investigation moves forward. Before doing so, therefore, you should contact your processor or a PCI forensic investigator (see below).

2. Identify a Lead Person. Regardless of the size of your organization, identify one person to lead the data breach response effort. This ensures that all information about the breach and strategies for "next steps" find their way to one, responsible person in your organization.

3. Retain Privacy Counsel with Experience in Data Breach Response. A complicated patchwork of federal and state laws now governs what steps businesses must take after learning that they have suffered a data breach. Indeed, most states require entities that suffer a data breach to notify potentially affected individuals, although the scope of that obligation and what information must be communicated to affected individuals varies considerably from jurisdiction to jurisdiction. It is therefore important to retain privacy counsel-with specific experience in data breach notification-to ensure that these requirements are followed.

Among other things, counsel should guide you on whether to notify (and precisely what to provide) potentially affected consumers, government agencies, law enforcement, and/or other third parties regarding the breach. Because communications with counsel are also protected from disclosure by the attorney-client privilege, retaining counsel gives you the ability to have candid conversations about liability risks associated with the data breach and steps to mitigate those risks. If you have insurance, your insurer may have a panel of law firms that you can choose from (see below for more information about insurance).

4. Notify Your Insurer (or Insurance Broker). Cyber insurance is increasingly common and may help cover the costs and potential liability associated with a data breach. Failure to notify your insurer promptly, however, can limit or undermine your coverage. Thus, whether through counsel or through your insurance broker, take steps to determine whether you have cyber insurance coverage and promptly notify your insurance company of a potential data-breach event. If you are planning ahead, check with your insurance broker about what type of cyber insurance coverage would be the best fit for your business because not all cyber insurance policies the same.

5. Work with Your Processor. Frequently, a notice from your processor will be the first you hear about a potential data breach at your location(s). Regardless of whether that is true in your case, be sure to work closely with your processor as soon as you learn that your payment systems have been (or may have been) compromised. Processors have a wealth of experience in responding to merchant data breaches and share your goal of minimizing liability exposure associated with any breach. Plus, if you don't already have a "backup plan" in place, your processor can help get your

ELECTRONIC TRANSACTIONS ASSOCIATION
Advancing Payments Technology

1101 16th Street, NW, Suite 402
Washington, DC 20036
800-695-5509

payments system back up and running quickly and safely, even while the investigation into the data breach continues.

In certain instances, your processor may inform you that it is "holding back" certain funds associated with your payment card transactions to address potential liability associated with a data breach. Critically, this does not mean that your processor has become the "enemy." Although dealing with such "holdbacks" can be difficult, your processor remains your best advocate for reducing potential exposure and minimizing risk.

6. Retain the Help of a PCI Forensic Investigator ("PFI"). Often times, the payment card brands will insist upon the retention of a PFI to investigate a potential data breach and ensure that the exposure has been contained. Even when that is not the case, promptly retaining a PFI-either directly or through legal counsel-is advisable to make sure that the breach, if any, has been eliminated.

You can find a list of PCI Certified Forensic Investigation Companies at https://www.pcisecuritystandards.org/approved_companies_providers/pci_forensic_investigator.php.

7. Take Remedial Action. Working with the PFI and your processor, promptly implement any recommended steps to ensure that the data breach has been stopped and that any system vulnerabilities have been properly remediated.

8. Implement a Communications Plan. Working with counsel, you should develop a plan for how to communicate about the data breach-both internally and with the media and other outside parties. This will include internal communication channels that preserve any applicable privileges, as well as methods of communicating accurate, but appropriately reassuring, messages to outsiders.

9. Document Your Response and Preserve Records. From data breach identification, to investigation, to remediation, be sure to carefully document the activities you are taking to contain and eliminate the data breach and preserve any records relating to the breach. Such records are not only useful to ensure that all appropriate actions are being taken to address the breach (in a sometimes hectic environment), but can be useful to minimize liability exposure associated with the data breach down the road. This documentation could be important in the event of litigation or a regulatory investigation by the Federal Trade Commission, state Attorneys General, or other authorities.

Data breach contact sheet ➔

This Nine Step Guide was prepared by the ETA's Risk, Fraud & Security Committee in collaboration with Arnall Golden Gregory LLP. The information contained herein is intended to provide general information to recipients regarding issues related to data breach response. It does not provide legal advice. Although the authors of the Nine Step Guide have gone to great lengths to make sure the information contained herein is accurate and useful, it is recommended that you consult with your lawyer if you are seeking legal advice.

ELECTRONIC TRANSACTIONS ASSOCIATION
Advancing Payments Technology

1101 16th Street, NW, Suite 402
Washington, DC 20036
800-695-5509

Data Breach Contact Sheet

Lead staff member _____

Phone Number (office)_____ Phone Number (cell) _____

Credit card processor _____

Phone Number _____ Merchant Number _____

Privacy Counsel _____

Phone Number _____

Address _____

_____

Property & Casualty Ins Co_____

Policy Number _____ Phone Number _____

Insurance Agent _____

Phone Number (office)_____ Phone Number (cell) _____

Data breach insurance _____
(if provided by your merchant processor)

Policy Number _____ Phone Number _____

PCI Vendor _____

Account number _____

Phone Number _____ Date last updated _____

Updated by _____

ELECTRONIC TRANSACTIONS ASSOCIATION
Advancing Payments Technology

1101 16th Street, NW, Suite 402
Washington, DC 20036
800-695-5509