

Top 10 Best Practices for Fighting Credit Card Theft and Fraud

Cyber criminals have a built-in advantage when it comes to compromising data. They think day and night about how to invent and execute a clever attack, and they gravitate to pathways that offer the least resistance for the greatest payoff. Many even work for organized crime syndicates.

Payment fraud can also strike close to home. A disgruntled employee with high-level access to internal financial systems and passwords could compromise the security of an entire organization.

Yet most companies don't have full-time security defense teams with the same intensity and focus on deterring hackers. The odds then, of a successful breach are in the hacker's favor.

Study after study shows that failure to protect sensitive payment data from a breach leads to massive financial costs, customer defections, lawsuits and loss of reputation. But by being equipped with the latest tools and techniques, organizations both large and small can effectively prevent and deter cyber fraud.

Managing the risk of a porous corporate perimeter has never been easy. As the economic world becomes more complex and payment fraud more prevalent, it's critical that companies arm themselves with tools and techniques that make cutting-edge fraud protection simple to use and effortless to manage.

Here are 10 tried-and-true best practices for protecting customer credit card account information and minimizing exposure to online payment scams:

1. The Best Defense is a Multilayered Offense.

Assume your company's computer systems will be compromised at some point and plan for it. No system on earth is 100 percent hack-proof, so manage the risk of a potential breach by solving for the concept of "graceful failure" – a deep, multilayered strategy that assumes perpetrators will eventually gain some form of access to your confidential data. If one safeguard fails, other countermeasures can detect and respond to

an attack by locking down payment data so it's worthless to hackers in case of a breach.

A good payment security system shouldn't merely detect intrusions. It should also have multiple deterrence layers that effectively complicate a breach attempt along with virtual padlocks on information access so there's less to steal if a thief does get in.

In your multilayered system, assign unique IDs to each person with computer access. Combine user IDs, passwords, and access tokens with tight, permission-based business rules around who needs to see or authorize confidential information, such as credit card types and accounts. Set very granular limits on transaction amounts and transaction velocity, as well as IP address protocols. Impose transaction restrictions on time of day and day of week, so that nothing and no one gets past your virtual front door outside normal working hours. Track and monitor all access to network resources and cardholder data, and ensure a detailed audit trail is created, so that you'll know who touched what data and when.

Think of this technology as a "Neighborhood Watch" for your computer network. It automatically sounds alerts for "things that don't belong"—out-of-pattern, unexpected events—whether they're intentional changes made by a system administrator or unintended, such as a failing hard drive or a malware attack. When the monitoring system finds anomalies, it sends up a flare, immediately notifying your IT staff that something is wrong—akin to police responding to a Neighborhood Watch emergency call.

2. Form an Incident Response Team.

To prevent a toxic data spill, assemble an internal "hazmat" team that thinks and works strategically to prevent and deter attacks rather than just detect them. Establish policies that address your company's information security requirements and processes, then share those policies with employees, suppliers and vendors so that everyone understands one another's goals, requirements and capabilities.

3. Use Your Head.

An alert mind is often the best defense against fraud. Train administrators and other users of your payment system to keep an eye out for unusual behavior – unexpected account usage, for example – and to sound an alert in case of anomalies.

Limit employee access to confidential cardholder data, since there's usually very little need for most company personnel to see or handle that data. Merchants who accept credit or purchase cards should set up their payment systems so that access is limited to key staff on a need-to-know basis.

Warn employees against clicking on pop-up windows or suspicious links in emails – even from people or businesses that appear legitimate – which can be tricks to install spyware and steal confidential information.

When using an online shopping cart, train employees and customers to look for safety symbols such as the padlock icon in a browser's status bar, "s" after "http" in the URL or the words "Secure Sockets Layer (SSL)" – all signs that a merchant is using a secure page for transmitting confidential information.

With social networking increasingly prevalent among today's workforce, establish guidelines for employee use of social media. Train personnel who update company blogs or access other social media sites to secure their privacy settings.

4. Lock Down System Gateways and Endpoints.

Protecting against malicious viruses, malware and spyware infections is often the first line of defense against a security breach. Your network architecture and PCs should be scanned frequently for vulnerabilities, every transaction point where payment information is exchanged should be scrutinized, and all payment data flows and touch points secured. Install antivirus and antispyware software from trusted sources and keep them updated with the latest patches.



CARD.VAULTSM

EC.NAVIGATORSM

EC.SENTRYSM

EC.ZONESM

EC.LINXSM

EC.BATCHSM

3Delta Systems, Inc. is a payment solutions company that delivers the power of secure, Internet-based purchase and credit card processing solutions to enterprise, business-to-business and business-to-government customers. 3DSI's complete suite of payment solutions - each designed from the ground up to be scalable, easy to implement and conform with PCI Data Security Standard best practices - enables merchants and buyers to manage, authorize and settle payment transactions in real-time.

3Delta Systems
14151 Newbrook Drive, Suite 200, Chantilly, VA 20151
P: 703.234.6010 | F: 877.408.7968 | www.3DSI.com

Automatically scan any flash drives or external hardware that connect to your network for viruses or malware. Never turn off your firewall, and have business policies in place for regular firewall maintenance. Use strong passwords and change them routinely.

5. Stay Informed.

When deciding on technologies for payment processing, be fluent in privacy protection as well as the 12 credit card protection and compliance requirements under the Payment Card Industry Data Security Standard (PCI DSS). By staying up-to-date, you'll be able to intelligently discuss the issues and decide on the countermeasures needed for your system as part of the sourcing team involved in payment technology acquisition.

6. Foster Awareness.

Stopping cyber crime begins and ends with individual computers and their users. Ensure all employees, contract personnel and business partners know your company's fraud policies, practices and fraud-response processes. Given the growing role of organized crime in perpetrating credit card fraud and theft, make sure anyone with access to important intellectual property and trade secrets is trained on the latest cyber criminal breach tactics, such as phishing, man-in-the-browser attacks and other social engineering schemes.

7. Adopt Industry Safeguards.

The major U.S. credit card companies developed the PCI standards as guidelines to help merchants, vendors, service providers and banks that collect, process and store credit card data protect it from being stolen or compromised. Becoming PCI-certified doesn't magically shield a business from losing data or provide impenetrable security against hackers or malware. However, the standards have proven to be an excellent roadmap for data security best practices. Use PCI DSS not only for card activity, but also as a roadmap for protecting access to other sensitive information, such as employee Social Security numbers or patient medical records.

8. Don't Collect What You Can't Protect.

One of the safest practices for businesses that process credit card data is so obvious it is often overlooked: eliminating the storage of that data altogether. No data stored = less risk. Unless it's absolutely necessary to retain payment or cardholder data, don't. Because credit card data must be secured at every point, complying with PCI rules as well as building and defending one's own data fortress can be extraordinarily difficult and prohibitively expensive. Organizations that collect and store that data for themselves often find the process to be a huge headache with potentially significant liabilities rather than a convenience for their customers. Transferring sensitive credit card and payment transaction data off site, where it is encrypted and stored at highly secure, PCI-compliant processing centers, is often the best solution.

9. Change the Target.

Tokenization is one of the best strategic weapons for protecting financial data. This process safely replaces a customer's real 16-digit credit card numbers or bank account data with a randomly generated string of characters called tokens, which then become useless to would-be hackers.

10. Do Your Outsourcing Homework.

When choosing an outside payment system or data security provider, make sure they have deep security capabilities and a like-minded business focus. If card-based, check that they're PCI-compliant, are audited every year by an independent third party and are Tier-1 certified. Tier-1 certification ensures that every feature, function and operational element of a company's services meets the highest levels of PCI data security. Does the provider offer the best combination of security, flexibility and ease of use for processing card payments? How often are logs that track user activity reviewed? Will audit trail analyses be readily accessible? Will the provider save you money by applying the lowest available credit card interchange rates when customer purchase transactions are accompanied by detailed, invoice-like information known as Level-3 line-item data? How robust is the provider's data centers that will house your customers' payment information? Seek a provider whose global payment platform and tokenization capabilities manifest a high degree of security, authentication and controls across all payment types and provides the mix of services you need with the most secure infrastructure and policies.

For more information, please contact
3Delta Systems at 703.234.6010,
sales@3DSI.com, or visit www.3DSI.com.

