

Ask the Attorney

Don't Compromise Your Customers' Identities

When guests pay by credit card, make sure their personal information is protected

Both Visa and MasterCard have information security standards that protect you and your customers from fraud. However, not all point-of-sale systems – and not all businesses' bookkeeping procedures – comply with these security standards. If you process transactions and capture data without compliant equipment or bookkeeping procedures, you may expose your customers to identity theft – and your business to thousands of dollars of fines.

In today's world, we continually read about information breaches. Hackers illegally access credit card information and capture data that lets them use cardholder information. Don't compromise your customers. Be ever vigilant in complying with security standards and safeguarding the information you obtain to process each credit/debit card transaction.

How Important Is It for You to Protect Your Customers?

Failing to comply with Payment Card Industry (PCI) Data Security Standards can cost you fines of up to \$500,000 and troubleshooting costs as high as \$100,000. Add to that the intangible cost of harming your customers and your business reputation.

Compliance is a really big deal, one you shouldn't have to handle alone. Be sure to partner with a credit/debit card processor who is focused on data security and compliance education.

Nine Ways to Protect Your Customers

Here are nine tips to help you better protect information obtained from credit/debit card transactions.

1 Consult with your card processor before making any changes to your point-of-sale system. If you're using a credit card payment software application or a point-of-sale terminal with a debit card PIN pad, you should ask your card processor to verify the compliancy and request an upgrade on outdated equipment or applications.

2 Build and maintain a secure network by using a POS system that complies with Visa's Payment Application Best Practices (PABP) and PCI Data Security Standards. To review Visa's list of validated applications, visit: www.visa.com/cisp.

Make sure you choose, install and maintain an up-to-date network firewall, antivirus and anti-spyware programs. These programs close holes in your network that hackers can use to gain entry and steal cardholder data. And always change the default password for your programs, firewall, routers, computers and other systems. This ensures only authorized persons can log on to your various network resources. Hackers know every product's default password. Their first line of attack will be to try to access your network using these well known logon credentials. If you change all of your passwords, this type of attack will fail.

3 Protect cardholder data by storing only the portion of customers' credit card data that is essential to your business – such as receipts and reports – in a secure area limited to authorized personnel only. Additionally, you should encrypt all transmissions across open, public networks. Encryption software is required for point-of-sale (POS) systems connected to the Internet for cardholder data transmission. Sensitive information, such as magnetic stripe data or card validation codes, should never be stored beyond what is required for business, legal or regulatory purposes.

4 Destroy all documents with obsolete transaction data that includes cardholder information. Each card association recommends a timeframe for retaining these kinds of documents.

5 Install and/or update your Internet firewall security on all computers and POS systems using IP connectivity – including those with dial-up Internet connections.

6 Implement access control measures. Only allow the most senior company officials to have access to cardholder data. Protect access by issuing user IDs and passwords and assigning access control rights through your network. Make sure everyone who will have access to cardholder data has had a background check performed and does not have a criminal record. Lastly, delete logons and update all company passwords when an employee leaves the company.

7 Regularly monitor and test your networks, and update your anti-virus software. This includes computers, POS systems and anything storing or processing cardholder data. Maintain tracking records to demonstrate your security systems

and processes are regularly tested and validated.

8 Enforce an information security policy. Document and maintain an enforceable policy that addresses details of information security. All employees handling sensitive information should know and understand the rules.

9 Report card theft immediately. A rapid response minimizes your risk and protects your customers.

Adopt Best-in-Class Processes

Making sure your equipment complies with Data Security Standards is essential. Just as important, make sure everyone in your company knows how diligent he or she must be to protect your customers. Make sure every employee follows these four processes.

1. Don't store any credit or debit card information when it is swiped unless the data is encrypted. Even then, store only the card's last four digits.
2. Don't print more than the last four digits of the card number on your customers' receipts. Never print the entire number. Some states, such as California, will soon be implementing new laws that allow only limited card number digits to be printed on the merchant receipt. Check with your attorney to ensure you comply with these state law initiatives.
3. Store your copy of each receipt in a safe, secure location.
4. Shred old receipts based on the timeframe recommended by each card association.

Choosing a Processor

Beyond due diligence, make sure your card processor is equally committed to protecting your customers' information. Not all payment processors are. As you evaluate a vendor, partner with one that fully supports PCI Data Security Standards.

Dennis Carpenter is the director of association alliances for Heartland Payment Systems, Inc. He can be reached at dennis.carpenter@e-hps.com. This information provided is general and educational and not legal advice. For additional information go to www.hospitalitylawyer.com.