Norris
McLaughlin
& Marcus, P.A.
Attorneys At Law

Business
Law Alert

April 2012

# Credit Card Security: How to Protect Your Business From Fees

If your business accepts credit or debit cards as payment from customers, you may be opening your company up to unexpected and costly penalty fees from credit card companies, acquiring banks or credit card processors for security violations.

Stephen and Cissy McComb, restauranteurs who ran a successful Italian eatery for over two decades in Park City, Utah, found themselves as just such unsuspecting parties. The McCombs were presented with claims from Visa and Mastercard totaling $1.26 million for alleged security violations, which they are currently battling in court. Specifically, the companies claimed that the McCombs (i) allowed charges from fraudulently used cards and (ii) violated security rules by keeping the data from too many customers' accounts. The credit card companies fined a middleman processing bank, which, in turn, pursued the McCombs for recoupment of the fines.

With such potentially steep fines, businesses are wise to revisit and evaluate their information security practices and understand just what categories of credit card information are off limits for storage.

As a starting point, it is important to note that the major credit card companies have imposed a Payment Card Industry Data Security Standard (the "PCI DSS") on every company that stores, processes or transmits cardholder information. The PCI lists twelve requirements for security compliance, which are further organized into control objectives as follows:

| Control Objectives | PCI DSS Requirements |
|---|---|
| Build and Maintain a Secure Network | Install and maintain a firewall configuration to protect card-holder data |
| | Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect Cardholder Data | Protect stored cardholder data |
| | Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program | Use and regularly update anti-virus software on all systems commonly affected by malware |
| | Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | Restrict access to cardholder data by business need-to-know |
| | Assign a unique ID to each person with computer access |
| | Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | Track and monitor all access to network resources and card-holder data. |
| | Regularly test security systems and processes |
| Maintain an Information Security Policy | Maintain a policy that addresses information security |

With respect to cardholder data, merchants are advised to store only the minimum amount of card data that is necessary to meet the needs of the business. Further, it is important to note that under the PCI, certain categories of a customer's credit card information should *never* be stored after authorization, including the following:

- Unencrypted credit card number
- CVV or CVV2 (card verification codes and values)
- PIN blocks
- PIN numbers
- Trace 1 or 2 data (magnetic stripe data)

Additionally, businesses should consider taking steps to avoid security compliance problems with credit card companies, acquiring banks, and credit card processors:

Review your contract with the credit card company, acquiring banks, and credit card processors, and any additional agreements and regulations that may apply (e.g. agreements or regulations referenced in any of the above contracts, including the PCI).

Consider your current security policies. Are they compliant with the PCI? Have you worked with outside PCI compliance consultants and/or do you regularly take the PCI Self-Assessment Questionnaires and conduct network vulnerability scans? (Note that each credit card company has different requirements based on the number of transactions you conduct annually. If you conduct a large volume of transactions, which for some credit card companies is over one million transactions, you may be required to have an annual onsite review by a security professional credentialed as a qualified security assessor (QSA). If you conduct a smaller number of transactions, it may be sufficient to complete an annual Self-Assessment Questionnaire and conduct regular network vulnerability scans by approved scanning vendors.)

Finally, keep in mind that compliance with the PCI, by itself, does not guarantee a business's safety. If this is a source of concern, consider additional protective measures such as internet insurance.

This *Business Law Alert* was written by **David T. Harmon** and **Grace H. Lin.** David is Co-Chair of the Executive Compensation and Employee Benefits Law Group, and Grace is an associate of the Business Law Group. If you have any questions regarding the information in this alert or any other related matters, please feel free to contact David or Grace by email at dtharmon@nmmlaw.com or ghlin@nmmlaw.com, respectively.

The *Business Law Alert* provides information to our clients and friends about current legal developments of general interest in the area of internet law. The information contained in this Alert should not be construed as legal advice, and readers should not act upon such without professional counsel.