LOCKE LORD LEGAL ISSUE Q&A Series

Heather Merton
Communications Manager
T: 617-239-0508
heather.merton@lockelord.com
www.lockelord.com

NOVEMBER 2015

"Retailers need to understand that these duties push down to every-one in their card chain, including third party vendors."

Mark E. Schreiber
Partner
Boston
617-239-0585
mark.schreiber@lockelord.com

Mark E. Schreiber's practice is in management defense of privacy, employment, and compliance matters, including internal company investigations involving data breaches, health care, anti-kickback, alleged fraud, financial improprieties, and other misconduct. He advises boards and special board committees on these matters.

Mark is a Certified Information Privacy Professional in the U.S. (CIPP/U.S.). He is also the Chair for Privacy Matters of the World Law Group, an international affiliation of 55 large law firms in some 73 countries. He was the recipient of the 2012 World Law Group Practice/Industry Group Leader of the Year Award in recognition of his privacy work.

Retailers: Beware of Pitfalls in Your Card Payment Function

Editor's Note: This is one in a continuing series of Q&As with Locke Lord lawyers on key legal issues confronting companies engaged in industries that have national and global impact.

What card payment rules must a retailer operating in the United States follow?

MS: When a merchant uses, transmits, stores or outsources the credit card function, it is subject to a number of rules in the U.S., including the Payment Card Industry Data Security Standard (PCI DSS). These rules change every few years and the new PCI DSS version, v. 3.1, issued April, 2015, is increasingly robust and encompassing. There are fines, penalties and assessments issued by the card brands for PCI non-compliance, for example, in the event of data breach. The rules touch every entity in the credit card ecosystem, from card processors to websites to hosting services to back-end storage — any company that stores or moves credit card information must comply and a detailed allocation of responsibilities is now required. Retailers need to understand that these duties push down to everyone in their card chain, including third party vendors. A merchant is still ultimately responsible under PCI rules for its third party vendor activities, including any outsourced card functions.

How do hackers take advantage of weaknesses in a retailer's technology?

MS: The hackers are smart and resourceful. They especially target systems with "low-hanging" fruit, including old code or that which is designed for functionality and speed, and not necessarily security. Recently some card breaches have also focused on third-party system vulnerabilities.

A new PCI DSS rule starting on July 1, 2015, which will become fully effective a year later, states that companies can no longer use Secure Sockets Layer (SSL), a security technology for establishing an encrypted link between a server and a client, to encrypt credit card data. SSL may no longer be used for any new card technology installations (with some limited exceptions), risk assessments are required, and companies must substitute a new system with more security. SSL has back-door vulnerabilities that hackers were able to exploit.

Are there specific U.S. laws concerning data collection and card payments during the point of sale?

MS: Yes. A number of U.S. state laws restrict collection of personal data in a credit card transaction at the point of sale (POS). These laws limit what personal data merchants can collect, such as ZIP codes and other personal identifiers, when running a credit card at POS in-store. There has been a boom in class action litigation in California and Massachusetts relating to this type of data collection, which merchants have followed closely. So far this litigation trend has been largely limited to these two states, and plaintiffs have been less successful in other states so far.

What can EU retailers learn from their American counterparts?

MS: Companies in the U.S. have experienced numerous card and other personal data breaches and now know how to deal with them. This experience in the U.S. extends to breach investigations, forensics, process management, remediation, notifications to government agencies and individuals, after-action follow-up, responses to regulatory enforcement actions and defense of class actions. The EU countries (and businesses there) so far do not yet have that level of practical or implementation experience because until recently data breaches, with some exceptions, did not have to be reported there.

Lessons learned from U.S. credit card data breaches are: secure your card data and frequently test it; compartmentalize and segregate your card data — don't store it when you don't need to; vet third party vendor's capabilities and security carefully; and consider updating incident response plans and cyberrisk insurance.

Locke Lord LLP disclaims all liability whatsoever in relation to any materials or information provided. This publication is provided solely for educational and informational purposes. It is not intended to constitute legal advice or to create an attorney-client relationship. If you wish to secure legal advice specific to your enterprise and circumstances in connection with any of the topics addressed, we encourage you to engage counsel of your choice. Attorney Advertising.

© 2015 Locke Lord LLP