

# Cyber Liability—International

Market Update Fall 2009



## Contact



**Emily Freeman**

Executive Director  
London, U.K.

Telephone: +44 (0)20 7933 2444  
E-mail: emily.freeman@uk.lockton.com



**Ben Beeson**

Executive Director  
London, U.K.

Telephone: +44 (0)20 7933 2857  
E-mail: ben.beeson@uk.lockton.com

The biggest data breach to date came to light at the beginning of the year regarding Heartland Payment Systems (HPY), the fifth biggest payment processor in the U.S. In the HPY Data Breach, 90 million credit cards were compromised resulting in significant losses to the insurance market.

HPY disclosed that intruders hacked into its network used to process 100 million payment card transactions per month for 175,000 merchants. At the time the company admitted that the intruders had access to Heartland's system for "longer than weeks" in late 2008. Tech security experts said the breach could set a record. Retail giant TJX lost 94 million customer records to hackers in 2007.

Although the insurance market remains competitive with plenty of carrier options and capacity, there has started to be some retrenching in the wake of Heartland as certain insurers stem their losses by cutting capacity and narrowing policy coverage.

At the same time, the regulatory and legal environment continues to tighten in the U.S.—at the beginning of 2009, as part of President Obama's stimulus package, the first federal notification law was introduced to the health care industry.

Two new rules have been created requiring health care organizations, and other entities that interact with personal health records (PHRs), to issue notifications in the event of a data breach. Both rules were created as part of the *American Recovery and Reinvestment Act of 2009* (ARRA), signed into law by the President in February.

An interim final rule, issued by the U.S. Department of Health and Human Services (HHS), requires health care organizations subject to *Health Insurance Portability and Accountability Act (HIPAA)* regulations to notify individuals whose information has been breached, when the breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals must be reported to the HHS annually.

A similar final rule issued by the Federal Trade Commission this week requires Web-based businesses that collect consumers' health information, including vendors and online applications that interact with PHRs, to issue notifications if a breach occurs.

Outside the U.S., the largest fine to date was levied by the FSA on HSBC Bank in the U.K. for £3m regarding lax company controls involving confidential and corporate personal data. The record fine resulted from the bank losing two unencrypted disks containing personal data in the mail, failing to store data securely, and poor staff training, it was alleged. It was reported that the fine could have been worse but for the firm's cooperation with the authorities, which got them a 30 percent discount on the fine.

This data breach has raised questions about whether the U.K. should pass a national data breach law, and already the Information Commissioners Office—the Government's Data Tzar—has been granted the power to raise greater fines on U.K. organizations that do not comply with the Data Protection Act.

Meanwhile, at the European Union level, the European Commission continues to look at imposing mandatory notification to affected groups in the same vein that exists in the U.S. The European Commission has proposed to amend the Directive on Privacy and Electronic Communications, commonly known as “the ePrivacy Directive.” If enacted, the proposed amendment to the ePrivacy Directive (a revised Article 4) would implement the first pan-European data breach notification requirement (though it has to be said it would be somewhat limited by U.S. standards).

Lockton's Technology Risks Team can assist you in controlling these evolving risks to your business from the management of your vendor program to advising on how to set up a security breach incident response plan. Traditional liability insurance has not kept pace with the regulatory and legal changes and Lockton, having identified the specific risks to your company, will design a quality insurance program where risk transfer is required.