MORRISON | FOERSTER

Legal Updates & News

Legal Updates

Privacy Report

March 2007

Related Practices:

- Financial Services Law
- Financial Services Litigation
- Litigation

No Breach Left Behind

Massachusetts is considering legislation (H. 213) that would require retailers to pay for losses that occur as a result of security system breaches. The Bay State bill is backed by bankers and would require retailers to reimburse banks for the costs of "reasonable actions" they take in response to a breach of data security, including cancellation or reissuance of credit cards, closure of accounts, stop-payments on checks, reopening of closed accounts, and any fraudulent charges made as a result of unauthorized transactions. If enacted, the bill would be the first such statute in the country, but a similar proposal may be introduced in Connecticut and at the federal level.

As if that won't grab the retailers' attention, consider California. Already home of the nation's first breach-notification law, the Golden State is toying with a bill introduced in February (A.B. 372) that would amend current law to let the Attorney General seek a civil penalty of up to $2,500 per violation of any of the law's data security, data disposal, and breach notification provisions. Under current law, individuals may sue to recover actual damages, but AG suits are limited to injunctive relief.

For more information, contact Tom Scanlon at tscanlon@mofo.com.

Maxx Mess

In January, retailer TJX Companies, Inc. announced that someone had hacked into its computer network that handles customer transactions for some 2,500 retail stores, resulting in the theft of personal credit, debit, and driver license information as far back as 2003. A week later, fraudulent use of the stolen information had been detected overseas. Banks have canceled hundreds of thousands of credit and debit cards. Numerous class action suits have been filed, including, in Canada.

One of the more intriguing filings is the class action by Alabama-based AmeriFirst Bank alleging common law claims of negligence, breach of contract, and negligence per se, as well as failure by TJX to adhere to the financial institutions' customer records privacy and data security safeguards rule of § 501 of the Gramm-Leach-Bliley Act. The class would include financial institutions (read, card issuers) that have lost money as a result of the TJX breach.

What's going on here? Class counsel are Alabama and Massachusetts plaintiffs' lawyers better known for bringing class actions against pharma over Fenphen, ephedrine, and other drug products. Why are these guys suddenly representing . . .banks? The complaint is also envelope-pushing. The GLBA and its implementing regulations do not provide a private right of action, and neither do most state data security statutes. But the negligence claim alleges that even though TJX may not be covered by the FTC's "safeguards" rules (16 C.F.R. Part 314), those rules establish a widely-accepted standard and, hence, a benchmark against which to assert a negligence claim.

For more information,contact Will Stern at wstern@mofo.com.

New York to World: "Watch Your SSN Digits!"

Watch out for New York's new Social Security Number Protection Law. The statute restricts the communication and use of Social Security numbers on or after January 1, 2008. What's the rub? The law defines a Social Security number as the number issued by the federal SSA *and any number derived from such number* (i.e., last 4 digits, etc.). The law prohibits intentionally communicating SSNs to the general public; providing an individual's SSN on any card or tag required for the individual to access products, services, or benefits provided by the entity; requiring an individual to transmit his SSN over the Internet unless the connection is secure or the number is encrypted; requiring an SSN to access a website unless another authentication device is also required; or providing an individual's SSN on any materials mailed except under certain limited circumstances. Even when an SSN can be mailed, the number may not be printed on a postcard or in a manner that would be visible without the envelope being opened.

The statute also requires companies to adopt reasonable measures to ensure that access is for a legitimate or necessary purpose related to the conduct of the business, and to provide safeguards against unauthorized access. The law exempts from its coverage the collection, use, and release of SSNs if required by federal or state law or the use for administrative purposes, internal verification, fraud investigation, or any business function authorized by the Gramm-Leach-Bliley Act.

For more information,contact Thomas Scanlon at tscanlon@mofo.com.

The Other Side of the Pond

The Brits just cranked up their data protection enforcement. Last week, the Government announced that it will introduce custodial sentences of up to two years' imprisonment for those found guilty of knowingly or recklessly obtaining or disclosing personal data from data controllers without their consent; or selling such personal data. This initiative follows from a recent series of custodial sentences ranging from eight months to two and a half years for those convicted of sending bogus notices demanding money to register under the Data Protection Act 1998.

For more information,contact Ann Bevitt at abevitt@mofo.com