

Recent developments in data security law in the United States

Lynne B. Barr and Jacqueline Klosek of Goodwin Procter LLP discuss the ChoicePoint and related cases and provide an insight into the possible implications for UK companies and international banks

A recent wave of publicity about data security breaches involving personal information of individuals in the United States has alarmed consumers already concerned about privacy and identity theft, prompted new regulation for banks from the federal regulators and fuelled frenetic legislative activity in many state legislatures and the US Congress.

The publicity surrounding the breaches has been driven in part by notices sent by US companies to consumers affected by the breaches as a result of such companies' efforts to comply with California legislation regarding notice of certain data security breaches. Disclosure of the breaches may also have been motivated in part by the efforts of public companies to comply with requirements of US securities laws.

ChoicePoint

The recent publicity started with the revelation of a massive data loss at ChoicePoint, one of the country's largest data brokers (companies that compile and sell publicly-available information about consumers, such as mortgage and real estate records, legal judgments and other government information). In early February 2005, ChoicePoint notified 46,000 California residents that the company had sold information concerning those residents to fraudsters posing as legitimate customers of the broker (it was later revealed that the breach actually affected up to 145,000 US residents). The company has since changed its enrolment practices to be more careful that its subscribers are legitimate businesses, but the damage was done.

Bank of America

Right on the heels of the ChoicePoint fiasco, in mid February 2005, one of the country's largest banks, Bank of America, revealed that it had lost tapes containing personal information on about 1.3 million cardholders, many of whom who also happened to be federal employees—including 60 US senators. Although the data was lost in December, there have been reports that Bank of America delayed sending notice to customers and mak-

ing public disclosure at the request of a law enforcement body. The bank has reported that there has been no evidence that any of the information has been used by identity thieves or otherwise.

LexisNexis

Following the highly publicized breaches at ChoicePoint and Bank of America, LexisNexis, another data broker and a subsidiary of UK-based publishing giant, Reed Elsevier Group plc, announced that it had experienced a security breach that had resulted in the theft of personal information of about 30,000 consumers, only to announce a few days later that, in fact, data on about 310,000 consumers had been stolen.

A new phenomenon?

The reports continue as this article is being prepared. A number of other enterprises, including Household Bank, DSW Shoe Warehouse and Ameritrade, have reported data breaches.

The massive publicity surrounding these recent breaches has prompted many to question whether this is a new phenomenon. The highly likely answer is 'no.' What has driven a relatively frequent but confidential occurrence in the world of financial and other databases to become front page and TV broadcast news in the US is a California law that passed relatively quietly in 2002, coupled with increasingly careful public company disclosures in the wake of the passage of sweeping corporate law reform by Congress in the form of the Sarbanes-Oxley Act, Pub. L. No. 107-204. This legislation, among other things, requires senior management certification of the effectiveness of internal controls and procedures for financial reporting and disclosures.

California's data security law

California is often the breeding ground for social change in America, and its passage of a law that requires companies that do business in California to notify affected consumers if unencrypted personal information

about them is accessed or stolen is an example. The scope of the law, codified at Cal. Civil Code §§ 1798.29, 1798.82-1798.84, is quite broad, as there is no definition of what constitutes “doing business” in the statute, and most companies, looking at California case law on the subject, have decided to err on the side of disclosure if they have customers in California, even if they have no physical presence there.

Personal information is defined in the statute relatively narrowly. It means a consumer’s first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social Security number,
- driver’s license or California identification number,
- account number or credit or debit card number,
- in conjunction with any security code, access code or password that would permit access to the consumer’s account.

The method of notification is specified in the statute. Generally, personal notice to the consumer is required, unless the number of consumers to be notified or the cost of such notice is too great; in that case, Web postings and general media notices can be sufficient. A company can delay notification at the request of a law enforcement agency, which is usually the US Secret Service when one is dealing with financial crimes.

Service providers to companies are required by the law to provide notice to the owners of the data if they become aware of unauthorized access to data that they are storing or processing. Additional guidance, in the form of “best practices” that elaborate on the statute’s provisions, has been provided by the California Office of

Privacy Protection (and can be found at <http://www.privacy.ca.gov/recommendations/secbreach.pdf>).

ChoicePoint found to its dismay that notifying only California residents is not a good idea. Its first notice went only to California consumers, but the media quickly picked up the story, and a number of state Attorneys General weighed in—arguing

that consumers in their states also deserved to receive notice. The trend now seems to be to tell all affected consumers.

New Bank Rules

In late March, US bank regulators issued joint guidance, published at 70 Fed. Reg. 15,736 (Mar.

29, 2005), on how banks in the US, including U.S. branches of foreign banks, need to handle data security breaches.

Banks are required to implement and maintain a response program for data security breaches. The required steps include prompt notification of the bank’s primary US regulator and law enforcement, remedial action to stop the breach and prevent its recurrence, and notice to affected customers if misuse of “sensitive customer information” is “reasonably possible.” Sensitive customer information is defined as the name, address or telephone number of the customer, in conjunction with a Social Security, driver’s license, account or card number or other information that would permit access to an account. Companies operating in the US other than banks are not yet subject to similar rules, but the Federal Trade Commission and other federal regulators, such as the Securities and Exchange Commission, could adopt similar rules under the same authority used by the banking regulators.

The Legislative Front

Nothing gets the attention of state and federal legislators like a newsworthy consumer problem, especially if the victims include legislators.

Numerous bills have been introduced in Congress to address the concerns raised by these disclosures. Some would ban the sale of Social Security numbers; others would provide for greater regulation of data brokers. And a California senator has introduced legislation patterned on the California law that would require notification to consumers. At this time, it appears likely that there will be federal legislation passed.

The enactment of new legislation at the state level also appears to be very likely. At present, California is the only US state with security breach notification legislation in place. California has proposed toughening its law to impose more stringent security breach notification requirements. As of April 1st, 2005, over 50 similar consumer notification bills had been introduced in at least 28 states, including Texas, New York, Washington, Minnesota, Illinois and Rhode Island. Legislation has passed in Georgia, North Dakota and Washington and is awaiting the signature of the states’ governors.

The sheer volume of legislative proposals, coupled with the speed with which such measures have been proposed, suggest that continued monitoring is clearly warranted. It is clearly more likely than not that several of the proposed measures will be enacted, at least at the state level. Thereafter, the main issue will become whether, and to what extent, the federal response to the issue will pre-empt state law, thereby protecting companies against having to also comply with numerous and potentially conflicting state laws.

Lynn B Barr
Jacqueline Klosek
 Goodwin Procter LLP
 lbarr@goodwinprocter.com
 jklosek@goodwinprocter.com

**“As of
 April 1st, 2005,
 over 50 similar
 consumer
 notification bills
 had been
 introduced in
 at least
 28 states.”**