FINANCIAL TIMES

WEDNESDAY 27 JUNE 2007

ID theft laws proliferate in the US

FT REPORT - CORPORATE SECURITY

BROOKE MASTERS

Stopping identity theft has become something of a public obsession in the US in the wake of the revelation earlier this year that electronic intruders had stolen credit card information for 45.7m separate accounts from the TJX company, a major retail chain.

Thirty-five states now have laws requiring companies to tell customers that their data has been compromised, and two other states and the District of Columbia have laws that will take affect in the next few months.

Twenty-two states have laws specifically governing the use of social security numbers, which are heavily used by financial services companies for identity purposes.

Many of the data breach and social security number laws actively contradict one another about which kinds of data are covered, and on how, when and to whom breaches should be reported. This raises real problems for national companies who have customers in many states.

At least four federal standards have been proposed in Congress, but so far none has passed, in part because of concerns that a weak federal law could pre-empt stricter state statutes and leave consumers worse off.

"I think we're stuck with a patchwork," says Jeff Marston, a partner with Powell Goldstein, a law firm. The US also lacks a national standard for data safety, leaving many companies scrambling to come up with security measures that could protect them not only from thieves but also lawsuits.

Seventeen states regulate the manner in which businesses dispose of personal information and at least six states, including California, have laws requiring companies to take steps to safeguard data. But most of the statutes are very unclear about the kinds of precautions they require.

"Nobody wants to specifically outline what (reasonable safeguards) mean because technology is moving too fast," says Alysa Zeltzer, a privacy and data security lawyer at Kelley Drye Collier Shannon.

In May, Minnesota becamethe first US state to impose financial penalties on companies that fail to adhere to a standard for keeping credit card information confidential, known as Payment Card Industry (PCI) Data Security Standard.

If a company fails to meet the PCI standard, which requires data to be disposed of within 48 hours, the firm pays any costs associated with a data breach. (Ordinarily card issuers pick up the tab.) California and Texas are considering similar legislation.

These new laws come at a time when many companies are struggling to comply with the 2003 Fair and Accurate Credit Transactions Act, which requires companies to dispose of credit card information in a timely manner and prohibits receipts from listing credit card numbers.

A recent survey by the Ponemon Institute found that half of all data breaches involved lost or stolen equipment such as laptops and memory sticks.

brooke.masters@ft.com