Class Action Litigation Report®

September 11, 2009

Privacy

Sprawling Identity Theft Case Raises Stakes for U.S. Firms, Attorneys Say

by Alexei Alexis

The Obama administration's recent announcement about an identity theft case believed to involve record amounts of stolen credit and debit card information points to an emerging trend of ever-larger break-ins that is causing legal headaches for businesses, several attorneys in the information security field told BNA.

The Department of Justice Aug. 17 announced that a Florida man, Albert Gonzalez, and two unnamed co-conspirators were indicted for allegedly hacking into computer networks supporting major U.S. retail and financial organizations and stealing data related to more than 130 million credit and debit cards (United States v. Gonzalez, D.N.J., No. 1:09-cr-00626-JBS, 8/17/09).

The DOJ said the case involved the largest alleged credit and debit card data breach ever charged in the United States.

High Stakes Seen for Businesses

Attorneys contacted by BNA following the DOJ announcement said the Gonzalez case is a clear indication that cybercrime has become a high-stakes problem for companies.

"I think we're going to see a lot more emphasis on data security as a legal obligation because of the kind of harm that people like this are able to do," said Thomas J. Smedinghoff, a partner in the data privacy and security practice at Wildman Harrold in Chicago. "The possibilities for fraud and malicious behavior are kind of endless."

Stewart Baker, a partner in the Washington office of Steptoe & Johnson LLP, said the case illustrates how much damage can be done by a few cybercriminals.

"I don't think industry has fully grasped the extent of its vulnerability," said Baker, a former assistant secretary for policy at the Department of Homeland Security. "If three punks can do this much harm, think of what could be done by a hostile nation."

Mark Rasch, co-founder of Secure IT Experts, a computer security consulting firm in Bethesda, Md., made similar observations.

"This shows that you don't need to be a foreign government or well-financed terrorist organization to do this kind of stuff," said Rasch, a former head of DOJ's computer crimes unit.

However, David Navetta, president of InfoSecCompliance, LLC, a data security and privacy law firm based in Denver, Colo., suggested that the importance of the case is debatable.

"It is pretty much a known fact that criminal elements, including organized crime, are after payment card data and personally identifiable information," he said. "There are online action forums where criminals can buy and sell credit card data."

Alleged Attack Viewed as 'Sophisticated.'

Among the corporate victims named in the Gonzalez indictment were Heartland Payment Systems, a New Jersey-based card payment processor; 7-Eleven, Inc., the Texas-based convenience store chain; and Hannaford Brothers Co. Inc., a Maine-based supermarket chain.

According to federal prosecutors, beginning in October 2006, Gonzalez and his co-conspirators researched the credit and debit card systems used by their victims; devised a sophisticated attack to penetrate their networks and steal credit and debit card data; and then sent that data to computer servers they operated in California, Illinois, Latvia, the Netherlands, and Ukraine.

The suspects are also accused of using sophisticated hacker techniques to cover their tracks and to avoid detection by their victims' antivirus software.

If convicted, Gonzalez faces as much as 35 years in prison, as well as fines of up to $500,000, the DOJ said.

He is currently in federal custody because of charges related to a previous hacking case, the department said.

In May 2008, the U.S. Attorney's Office for the Eastern District of New York charged Gonzalez for his alleged role in the hacking of a computer network run by a national restaurant chain.

Trial on those charges is scheduled to begin in September, DOJ said.

In August 2008, Gonzalez and others were indicted for hacking incidents targeting TJX Companies Inc. and other major retailers and involving the theft of data related to 40 million credit cards. At the time, the DOJ said the case set the record for the biggest identity theft scam charged in the country.

Gonzalez is scheduled to be tried in 2010 for those charges, which were filed in the District of Massachusetts.

The latest case is being prosecuted by Assistant U.S. Attorneys Erez Lieberman and Seth Kosto for the U.S. Attorney's Office for the District of New Jersey and by Senior Trial Counsel Kimberly Kiefer Peretti of the Criminal Division's Computer Crime and Intellectual Property Section, the DOJ said. The case is being investigated by the U.S. Secret Service, the department said.

Banks Worried About Breach Costs

With the size of data security breaches steadily growing, banks are increasingly demanding to be reimbursed by retailers and other third parties for breach-related "clean-up" costs, such as the expense of reissuing cards, according to Randy Sabett, a partner in the Washington office of Sonnenschein Nath & Rosenthal LLP.

"Historically, when a breach occurs, the entity left holding the bag is the financial institution," he said. "They're now turning to the courts to recover the costs."

Depending on the number of customers involved and whether fraudulent charges were made, breach-related costs could potentially be huge for the industry, Smedinghoff said.

In 2007, TJX disclosed that its computer network was hacked into and that tens of millions of payment cards were compromised. The company ended up paying about $70 million to settle bank-related class action lawsuits.

The banks alleged that TJX had failed to comply with the Payment Card Industry Data Security Standard (PCI DSS), which requires merchants, their banks, and credit card transaction processors to build and maintain a secure computer network, maintain a vulnerability management program, and regularly monitor and test networks.

Heartland Discloses Legal Issues

At least one of the companies in the latest case appears to be facing similar legal troubles. In a March Securities and Exchange Commission filing, Heartland disclosed that it was grappling with 22 class actions related to a data security breach discovered in January, including 17 consumer complaints, four complaints filed by banks, and one investor complaint.

The company also revealed that the Federal Trade Commission and several state attorneys general were investigating the incident.

In June, TJX agreed to pay nearly $9.8 million to a group of 41 state attorneys general to end their investigation into the company's 2007 data breach, according to court documents (In re TJX Cos. Inc., Mass. Super. Ct., case number unavailable, 6/23/09).

The retailer was required to pay $5.5 million to the states for their use in general consumer protection efforts, $2.5 million to a "Data Security Trust Fund" to be used by the AGs for consumer personal information protection enforcement and policy efforts, and $1.75 million to cover costs incurred by the states in investigating TJX.

Under the agreement, TJX was also required to implement extensive data security measures to protect personal information.

TJX had already agreed to improve its data security practices under a March 2008 agreement with the FTC. The pact required the firm to implement a comprehensive security program reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers, and to obtain audits by independent third-party security professionals every other year for 20 years.

New Regulations Expected

Meanwhile, Smedinghoff said the growth of cyber attacks in recent years is also generating a patchwork of state laws and is ultimately likely to result in federal legislation.

Dozens of states have already passed laws requiring companies to notify consumers affected by data security breaches.

In a new trend, states such as Nevada and Massachusetts have begun "edging into substantive security regulation," Baker said, adding that further security regulation is inevitable.

"The real question is whether we get piecemeal regulation or federal rules, or both," he said. "In my view, we would be better off with federal rules."

Congress has struggled to enact data security legislation, despite broad, bipartisan support for addressing the issue. In the previous two Congresses, conflicting data security bills were introduced, and several congressional committees claimed jurisdiction over the issue, complicating the path to final passage.

Federal Bills Pending

Senate Judiciary Chairman Patrick Leahy (D-Vt.) is among members of Congress who have continued to push for the enactment of federal data security legislation.

In July, Leahy reintroduced a comprehensive data security bill (S. 1490), saying that final passage is among his "highest legislative priorities."

The measure would require businesses that maintain personal information on consumers to establish data security programs and to notify individuals affected by a security breach, unless a risk assessment concludes there is "no significant risk" of harm to consumers. Companies would have to provide the risk assessment to the Secret Service.

The House Energy and Commerce Committee is considering a similar bill (H.R. 2221). That legislation, introduced by Reps. Bobby L. Rush (D-Ill.) and Cliff Stearns (R-Fla), would require the FTC, within one year of the measure's enactment, to promulgate data security standards for

all businesses engaged in interstate commerce. The commission would be prohibited from requiring the use of specific technologies.

Also, in the event of a data security breach, companies would be required to notify affected consumers, unless there is "no reasonable risk of identity theft, fraud, or other unlawful conduct."

In June, the House Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection passed the bill by voice vote, and it now awaits full committee action.

Views on Industry Standards Mixed

When asked whether the Gonzalez case points to the inadequacy of industry standards, experts offered mixed opinions.

Pam Dixon, founder of the World Privacy Forum, a public interest group based in California, said the standards probably need to be reviewed.

"What this case represents is the maturity of the criminals in this field," she said. "Businesses are going to really need to rethink what they've been doing. Just plucking the low-hanging fruit will not be enough going forward."

However, others said that existing industry standards appear to be working for the most part.

"I don't see this as a criticism of the standards," Sabett said. "They could probably use some tweaking here and there, but there is also the question of whether there has been adequate compliance."

In addition, he noted that there is currently a controversy brewing over the adequacy of qualified security assessors (QSAs), who are responsible for determining whether firms are PCI-compliant.

"It's a question of who is watching the watchers," he added.

The PCI Security Standards Council, which oversees the industry rules, has stood by them, despite facing criticism in the wake of recent breaches.

"It is important to remember that compliance validation is a snapshot in time," Bob Russo, general manager of the council, said in an e-mail. "As such, companies like TJX and Heartland could very well have been compliant on the day its QSA wrote its assessment report. But if subsequent logging rules were not followed, patches were delayed, or scanning wasn't performed on a regular basis, the company may have no longer been compliant."

Offering support for the standards, Rasch said they are only designed to provide a minimum, flexible set of protocols.

"The goal of the standards is not to absolutely prevent an attack," he said. "The goal is to provide a basic level of security. The question with federal legislation is: Will it specify exactly what security measures you need to take?"

Lisa Sotto, a partner at Hunton & Williams, New York, raised similar concerns.

"The difficulty is that you can't prescribe specific standards because of the speed with which technology changes," she said. "But it is possible to legislate some basic security standards, for example, requiring entities to put in place appropriate safeguards in light of their own operations and data."

Sabett said that what might be helpful, from a business perspective, is the passage of a federal data breach notification law that preempts the existing patchwork of state laws.

"It all depends on what it looks like," he said.

Among other priorities, business groups are seeking a federal data breach law that requires notification to consumers only when there is a risk of identity theft, ideally a "significant" risk. They are also pushing for complete preemption of state laws.
Dixon agreed that a federal breach law would be useful. However, she said it was important that Congress not pass a weak law that removes stronger protections at the state level.

Whether Congress is finally ready to enact data security legislation remains to be seen, observers said.

"I think Congress will be busy with health care and other issues for a while," Dixon said. "If we see more Gonzalez cases over the next year or two, I suspect that Congress will eventually get involved. But my sense at this point is that industry is more motivated than Congress to do something about this."