InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Secret Service Busts Four Fraudsters With Ties To T.J. Maxx Attack

The South Florida bust resulted in the recovery of about 200,000 stolen credit card account numbers used in fraud losses roughly calculated to be more than $75 million.

By Larry Greenemeier, InformationWeek
July 12, 2007
URL: http://www.informationweek.com/story/showArticle.jhtml?articleID=201001100

A recent Government Accountability Office report noted the difficulty of linking data theft to identity theft, but the U.S. Secret Service is having no such problems. The agency earlier this week said it has arrested and indicted four members of an organized fraud ring in South Florida, charging each of them with aggravated identity theft, counterfeit credit-card trafficking, and conspiracy. And the Secret Service has been able to trace the origin of the data used to perpetrate this identity theft and fraud back to the theft of millions of customer records from T.J. Maxx parent company TJX and from Polo Ralph Lauren.

The South Florida bust resulted in the recovery of about 200,000 stolen credit card account numbers used in fraud losses roughly calculated to be more than $75 million. Agents also seized two pickup trucks, $10,000 cash, and one handgun in connection with the case.

TJX reported late last year that it suffered an unauthorized intrusion or intrusions into portions of its computer system that process and store information related to credit and debit card, check, and no-receipt merchandise return transactions. This admission that customer information -- more than 45 million records -- was stolen from some stores dating back to 2003 opened the floodgates to lawsuits from store customers afraid of identity theft and from financial institutions whose customer service costs have increased as a result of worried clients. Polo Ralph Lauren in April 2005 suffered a data breach through which 180,000 customer records were exposed.

TJX claimed in a June regulatory filing that it does not know "who took this action, whether there were one or more intruders involved, or whether there was one continuing intrusion or multiple, separate intrusions." TJX has already spent $20 million, or 0.5% of net sales for the quarter, related to the intrusion. The money has gone toward investigating and containing the computer intrusion, improving the company's computer security and systems, communicating with customers, and technical, legal, and other related costs, the company stated.

Law enforcement continues to chip away at the mystery. The Secret Service's Miami Electronic Crimes Task Force, working with the agency's Nashville field office, earlier this year arrested a 30-year-old Florida man -- who used the online handle "Blinky" -- and his girlfriend. Blinky is accused of trafficking counterfeit credit cards and identifications for years over the Internet. His arrest turned up evidence of an organized fraud ring involving Cuban nationals operating in South Florida and led to the four arrests and indictments announced this week. The fraudsters were sending large amounts of money via E-Gold accounts to known cybercriminals in Eastern Europe in return for tens of thousands of stolen credit card account numbers. The stolen credit card account numbers were then used to counterfeit credit cards in "plants" throughout southern Florida, the Secret Service said in a statement.

Law enforcement has been critical of E-Gold for acting as a conduit for money flowing into criminal enterprises. A federal grand jury in late April indicted E-Gold, Gold & Silver Reserve, and the owners of these digital currency businesses on charges of money laundering, conspiracy, and operating an unlicensed money transmitting business.

However, E-Gold chairman Douglas Jackson disputes these charges and asserts that his company first brought Blinky to the attention of law enforcement in March 2006. Jackson told *InformationWeek* that investigators working for E-Gold began monitoring Blinky pursuant to an undercover operation it was conducting with law-enforcement agents from the U.S., U.K., and Russia. "In May 2006, working with records supplied by an exchange service that had sold him some E-Gold, we were able to supply general location (Miami), three confirmed phone numbers he used, and the usual IP/timestamp combos that even in this day and age are often useful," Jackson said.

This isn't the first time that customer data stolen from TJX has been used to commit fraud. In March, the Florida Department of Law Enforcement confirmed TJX customer data was used to make the fake credit cards that were used to purchase about $8 million in Wal-Mart and Sam's Club gift cards. The fraudsters hit stores in 50 of Florida's 67 counties.

All of this has meant headaches for TJX. In March, the company received a civil investigative demand from the Massachusetts Attorney General's office seeking documents about the computer intrusion that led to the theft of customer data. This was followed by similar demands from other states' attorneys general. TJX is also being sued by customers, financial institutions, and shareholders.

The TJX data breach may have worst-case-scenario written all over it, but "there's nothing different about TJX that couldn't have happened to someone else," Joshua Levine, managing director of Kita Capital Management and former CTO for E*Trade, told *InformationWeek*. "Everyone's just glad that it didn't happen to them."

The GAO's report aside, all companies should be more concerned about how they protect their customer data. "On a small scale, I think every corporation is comfortable that identity theft can and does happen, but as long as it happens on a small scale, it's a cost of business," Levine said, adding that TJX could ultimately be the case that changes all of this. "TJX is a turning point where we could turn it into a triumph rather than a disaster."