**TJX case study**

TJX hack has been known as the biggest breach of personal data. The figures are astounding US securities Exchange commission filings by the firm show that 45.7 million credit and debit card numbers were stolen over a period of 18 months. TJ Maxx alone has spent $130 million dealing with the aftermath of the intrusion. The consultant retained by TJX to investigate the breach found that the company had not complied with nine of the twelve security measures mandated by credit-card companies under the Payment Card Industry (PCI) Data Security Standard (DSS), the court documents stated.

The breach, originally disclosed by TJX in January, has led to widespread credit- and debit-card fraud in at least 13 countries, surpassing $68 million for Visa cards alone, according to one executive's deposition. Stores in Canada and the United States have reported fraud, and a ring of fraudsters in Florida had used credit-cards stolen from TJX to purchase more than $8 million in gift cards.

According to the court documents, in July 2005, the data thieves compromised TJX's network by breaking into the wireless network of a store in Florida. Attackers gained access to the wireless network in a marshall’s discount clothing store in Miami, Florida. Over the next year, the internal network systematically searched for the valuable information.

In May 2006, the intruders placed a traffic sniffer on the company's internal network, capturing sensitive cardholder information that had been transmitted without encryption. The information included large amounts of sensitive card-specific data known as Track 2 Data. Track 2 data includes account numbers, expiration dates and encrypted personal identification numbers, plus other information that card-issuing banks can include at their discretion. Retailers are forbidden from storing such information under the Payment Card Industry (PCI) Data Security Standard being pushed by Visa, MasterCard International Inc. and other credit card companies. But many retailers continue to do so, often because their point-of-sale systems capture and store the data by default.

"Track 2 Data is extremely sensitive because, if it is compromised, it is simple to create a counterfeit payment card from the compromised data," the banks maintained in their court filing.

December 2006, one of the incidents that may have led to the firm's discovery of the breach was reports sent to TJX in November 2006 by law enforcement officials in Florida who had uncovered a ring of thieves using credit card stolen from the retailer to carry out fraudulent transactions. Six people have been jailed in connection to those crimes, and another four people currently are wanted by the Florida Department of Law Enforcement. the incident was discovered by the TJX. Even after the exhaustive investigation that TJX has employed since first discovering the attack on Dec. 18, 2006 -- including the hiring of computer forensics specialists from IBM and General Dynamics -- the firm admits it may never know the full scope of the data loss.

Accused:

**Stephen Watt**, 25, allegedly customized a packet-sniffing program called "blabla" for use by **Albert Gonzalez**, a former Secret Service [informant](https://www.wired.com/27bstroke6/2008/08/indicted-federa.html) who was [indicted](https://www.wired.com/27bstroke6/2008/08/11-charged-in-m.html) earlier this year as the mastermind of a 2005-2007 intrusion into clothier T.J. Maxx, as well as breaches at BJ’s Wholesale Club, Boston Market, Barnes & Noble, Sports Authority, Forever 21, DSW and OfficeMax.

Gonzalez allegedly used sniffers to scoop up credit and debit card numbers from hacked networks as they sped from cash registers to processing servers. Watt modified blabla "on diverse dates" to meet Gonzalez's evolving needs, according to the one-count [federal information](https://www.wired.com/images_blogs/threatlevel/files/steven_watt_information.pdf) (.pdf) filed in federal court in Boston on Wednesday.

Watt is charged with conspiracy to commit computer fraud, wire fraud, identity theft and money laundering.

Ten other defendants have previously been charged with Gonzalez in the hack attacks. Last month one of them, **Damon Patrick Toey** of Miami, pleaded guilty and [agreed](https://www.wired.com/images_blogs/threatlevel/files/toey_plea.pdf)(.pdf) to cooperate against the other defendants in exchange for a recommendation of a reduced sentence.

Toey was released to electronic monitoring, then nearly returned to jail when his pretrial services officer [discovered a computer in his home](https://www.wired.com/images_blogs/threatlevel/files/toey_computers.pdf) (.pdf), in violation of his release conditions. When Toey had the computer removed to a storage unit, he was allowed to remain free pending sentencing, currently set for December.