**The Worst Data Theft Ever**

On August 17, 2009, 28 year- old Alberto Gonzalez of Miami was charged along with two Russian accomplices with carrying out the largest hacking and identity theft crime in U. S. history. Federal prosecutors alleged that the three had masterminded a global scheme to steal more than 130 million credit and debit card numbers between 2006 and 2008 by hacking into the computer systems of companies that included the Hannaford Bros. supermarket chain, 7- Eleven, and Heartland Payment Systems, a credit card processing company. The group used a network of computers in New Jersey, California, Illinois, Latvia, the Netherlands, and the Ukraine to infiltrate the computer systems of targeted companies, using sophisticated techniques to evade detection by antivirus software. They planted software programs in these companies’ computer net-works that enabled them to steal more data in the future as well as “sniffer” programs to capture card data while they were being transmitted between computer systems. An unspecified number of the stolen credit and debit card numbers were sold online and used to make unauthorized purchases and withdrawals from banks. Gonzalez and his group have been responsible for other major data thefts as well. On September 18, 2009, Gonzalez pleaded guilty to 19 counts of criminal activity and credit card fraud in attacks against Barnes and Noble, OfficeMax, Boston Market, and Sports Authority. Gonzalez was also responsible for stealing 40 million credit and debit card numbers from TJX Cos., the parent company of T. J. Maxx. The data thefts at Hannaford, Heartland, and 7- Eleven Stores were carried out using SQL injection attacks, which we defined earlier in this chapter. SQL injection attacks are well understood, and security experts have warned retailers about them for years. Nevertheless, many companies still use older versions of Microsoft SQL Server database management software that allow attackers to take control of the database with a SQL injection. Gonzalez and his ring started using SQL injection attacks around August 2007. Before that time, they penetrated corporate systems by exploiting weak wire-less security. The thieves drove around and scanned retailers’ wireless networks to identify network vulnerabilities and then installed sniffer programs that tapped into the networks for processing credit cards, intercepting customers’ debit and credit card numbers and PINs (personal identification numbers). These techniques enabled the group to siphon off more than 40 million credit and debit- card numbers from TJX in July 2005. Gonzalez’s team identified a vulnerable network at a Marshall’s department store in Miami and used it to install a sniffer program on the computers of the chain’s parent company, TJX. The group was then able to access the central TJX data-base, which stored customer transactions for T. J. Maxx, Marshalls, HomeGoods, and A. J. Wright stores in the United States and Puerto Rico, and for Winners and HomeSense stores in Canada. TJX was still using the old Wired Equivalent Privacy (WEP) encryption system, which is relatively easy for hackers to crack. Other companies had switched to the more secure Wi- Fi Protected Access (WPA) standard with more complex encryption, but TJX at that time had not made the change. An auditor later found that TJX had also neglected to install fire-walls and data encryption on many of the computers using the wireless network, and didn’t properly install another layer of security software it had purchased. TJX acknowledged in a Securities and Exchange Commission filing that it transmitted credit card data to banks without encryption, violating credit card company guidelines. TJX also retained cardholder data in its systems much longer than stipulated by industry rules for storing such data. In March 2008, TJX management agreed to strengthen the company’s information system security. It also agreed to have third- party auditors review security measures every 2 years for the next 20 years. TJX has already spent over $ 202 million to deal with its data theft, including legal settlements. Forrester Research estimates that the cost to TJX for the data breach could surpass $ 1 billion over five years, including costs for consultants, security upgrades, attorney fees, and additional marketing to reassure customers. Hannaford Bros. also started implementing additional security safeguards. It updated firewalls, installed a round- the- clock security monitoring and detection service from IBM, and also began encrypting traffic flowing over a private network from its store registers to its credit card processor. (The existing Payment Card Industry Data Security Standard [PCI DSS] guidelines, which apply to all companies processing credit cards, only require encryption of data transmitted over public networks.)