



THIS STORY HAS BEEN FORMATTED FOR EASY PRINTING

## Advanced tactic targeted grocer 'Malware' stole Hannaford data

*The Boston Globe*

By Ross Kerber, Globe Staff | March 28, 2008

A massive data breach at Hannaford Brothers Cos. was caused by a "new and sophisticated" method in which software was secretly installed on servers at every one of its grocery stores, the company told Massachusetts regulators this week.

The unauthorized intrusion the company disclosed on March 17 stemmed from software that intercepted card data from customers as they paid with plastic at store checkout counters, and sent the data overseas, Hannaford's top lawyer said in a letter sent to Attorney General Martha Coakley and Governor Deval Patrick's Office of Consumer Affairs and Business Regulation.

The software was installed on computer servers at each of the roughly 300 stores operated by Hannaford and its partners. Hannaford did not say how the software might have been placed on so many servers, and company spokeswoman Carol Eleazer said the company continues to investigate how the software was installed and other specifics of the breach. The Secret Service, which pursues currency crimes, is conducting its own investigation.

Data security specialists say the new details show how hackers have grown more adept at penetrating weak links in the systems that connect merchants and banks. In previous breaches, such as the record-setting intrusion at TJX Cos. of Framingham, where as many as 100 million card numbers were compromised, hackers took advantage of merchants who stored customer names and card data - sometimes in violation of payment industry standards - at central locations in their computer networks.

In contrast, Hannaford says it did not store customer information. The hackers who struck Hannaford mined a stream of data that the merchant and banks were not responsible for protecting under industry rules, industry specialists said.

The Hannaford breach "was markedly more sophisticated," said Steve Rowen, a partner at Retail Systems Research of Miami, which does consulting work for merchants.

The Hannaford breach also poses worrisome questions for the payment industry as it struggles to tighten security. Hannaford, for example, had met compliance standards set by Visa Inc. and other card companies, but that did not stop the breach.

"Just because they are compliant, it doesn't mean they are safe," said Graham Cluley, technology consultant for Sophos Inc., a Burlington computer security firm. Card issuers and others need to find other ways to improve security, he added.

"Clearly, consumer confidence is being shaken by this constant stream of breaches," Cluley said.

Hannaford said in the letter that the problem potentially compromised the account numbers and expiration dates on all 4.2 million credit and debit card numbers used at its stores in six states between Dec. 7 and March 10, though the actual number taken may be smaller. Hannaford said it knows of about 2,000 cases of fraud related to the intrusion.

Hannaford's letter was sent by its general counsel, Emily D. Dickinson.

Dickinson wrote that an "illicit and unauthorized computer program" known as "malware" was installed on the servers of each of the stores the company operates in Maine, Vermont, New Hampshire, Massachusetts, and New York, plus at stores elsewhere, including the Sweetbay chain in Florida, that use its payment systems.

Hannaford and Sweetbay are owned by Belgium's Delhaize Group.

The malware intercepted the "track 2" data stored on the magnetic stripe of payment cards as customers used them at the checkout counter, Dickinson wrote. This track includes the card's number and expiration date, but not the customer's name.

The data were taken "in transit for authorization from the point of sale," the letter states, meaning as it was transmitted from the cash register to one of the institutions that Hannaford uses to process transactions. Eleazer said these include major card networks and First Data Corp. of Denver, a major processor.

The malware on the store servers stored up records of these purchases in batches, then transmitted them to an unnamed offshore Internet service provider, the letter states. Foreign crime rings have been blamed in a number of other payment card fraud cases.

"Law enforcement officials and others report that the method of illicit acquisition is a new and sophisticated method in that it obtains data in transit during the course of the authorization process," the letter states.

Cluley said the software could have been installed remotely. This could have been accomplished through a breach of the company's firewall. Alternatively, the servers may not have been running the latest security patches, or may have had antivirus programs that weren't updated. Hannaford stated in the letter that it has replaced the hardware on which the malware was installed. Cluley said that could suggest a company insider or a technician for one of its vendors could have placed the code.

Executives of Visa Inc. of San Francisco, the largest payment card company, issued a statement yesterday saying it is working with Hannaford, banks, and law enforcement.

Hannaford said in its letter that it was certified a year ago as meeting card security standards and was recertified on Feb. 27. Eleazer said that was the day Visa first notified Hannaford of unusual card activity and began its investigation. That the standards did not stop the thieves, she said, "speaks to the increasing sophistication of the criminal element that propagates these attacks," she said.

*Ross Kerber can be reached at [kerber@globe.com](mailto:kerber@globe.com). ■*

© [Copyright](#) 2008 The New York Times Company