

# Hannaford Bros Supermarkets & Sweetbay Stores Hit By Big Data Breach

March 18, 2008

## Were You Affected By The Breach? Your Friends & Family?

A security breach at an East Coast supermarket chain exposed 4.2 million credit and debit card numbers and led to 1,800 cases of fraud, the Hannaford Bros. grocery chain announced Monday.

Hannaford said credit and debit card numbers were stolen during the card authorization process and about 4.2 million unique account numbers were exposed.

The breach affected all of its 165 stores in the Northeast, 106 Sweetbay stores in Florida and a smaller number of independent groceries that sell Hannaford products.

The company is aware of about 1,800 cases of fraud reported so far relating to the breach.

No personal data such as names, addresses or telephone numbers were divulged -- just account numbers.

Hannaford became aware of the breach Feb. 27. Investigators later discovered that the data breach began on Dec. 7; it wasn't contained until March 10, said Carol Eleazer, Hannaford's vice president of marketing in Scarborough.

"We have taken aggressive steps to augment our network security capabilities," Hannaford president and CEO Ronald C. Hodge said in a statement released Monday. "Hannaford doesn't collect, know or keep any personally identifiable customer information from transactions."

The company urged its customers to monitor their credit and debit cards for unusual transactions and report any problems to authorities.

The U.S. Secret Service, whose duties include investigating electronic crimes such as data breaches, confirmed it's investigating but declined to comment on the scope of the crime.

"The company did contact us, and we are investigating," said agency spokesman Malcolm Wiley.

MasterCard, the second-biggest U.S. credit card association after Visa, issued a statement before Hannaford's disclosure: "Because this incident is the subject of an ongoing law enforcement investigation, we cannot disclose additional details regarding the incident or otherwise comment at this time."

Calls to Visa were not returned.

Mark Walker, an attorney for the Maine Bankers Association, said his organization sent an advisory to member banks Friday after learning of the breach. Only a few had reported suspicious activity involving the credit and debit cards they had issued customers, Walker said.

"I had expected there would be more than we've heard of," Walker said. "But it's still too early for us to tell."

Bruce Spitzer, a spokesman for the Massachusetts Bankers Association, criticized the delay in public notification of the source of the breach.

"Visa and MasterCard have stipulated in their contracts with retailers that they will not divulge who the source is when a data breach occurs," Spitzer said. "We've been engaged in a dialogue for a couple years now about changing this rule.... Without knowing who the retailer is that caused the breach, it's hard for banks to conduct a good investigation on behalf of their consumers. And it's a problem for consumers as well, because if they know which retailer is responsible, they can rule themselves out for being at risk if they don't shop at that retailer."

Paul Stephens, of the San Diego-based consumer advocacy organization Privacy Rights Clearinghouse, said the delay in disclosure "puts consumers in a difficult position because they have no way of knowing whether their accounts may have been impacted or not."

Eleazer defended Hannaford's actions.

"We moved with all deliberate speed to get out to customers with information that we could have confidence in," she said. "This is a complex undertaking."

Consumer advocates said this crime costs \$50 billion each year. And while victims aren't held responsible for fraudulent charges, in the end everyone pays.

"At the end of the day, as customers, we all pay for it because we get that passed on to us in the form of higher costs for consumer goods and products," said Eric Bourassa with **MASSPIRG**.

