

» Cars » Auto Financing » Event Tickets » Jobs » Real Estate » Online Degrees » Business Opportunities » Shopping

Search

How do I find it?

Subscribe to paper

Advertisement

3M
Privacy Filters

KEEP WANDERING EYES OFF YOUR LAPTOP

BUY NOW



Home News Travel Money Sports Life Tech Weather

Technology Products Science & Space Gaming Wi-Fi Center

Supermarket breach exposes 4.2M accounts

Posted 19h 38m ago | Comments 6 | Recommend 3

E-mail | Save | Print | **RSS**

By David Sharp, Associated Press

PORTLAND, Maine — A security breach at an East Coast supermarket chain exposed more than 4 million 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 card numbers were exposed, placing the case among the largest data breaches ever.

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.

FIND MORE STORIES IN: [Florida](#) | [Boston](#) | [Northeast](#) | [East Coast](#) | [Walker](#) | [Visa](#) | [Mastercard](#) | [Mass.-based Framingham](#) | [Marshalls](#) | [Scarborough](#) | [TJX Cos](#) | [Massachusetts Bankers Association](#) | [Malcolm Wiley](#) | [San Diego-based Privacy Rights Clearinghouse](#) | [Sweetbay](#)

"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. It also told customers to beware of e-mails and calls from people claiming to represent Hannaford and seeking any personal information.

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.

Beth Givens, director of the San Diego-based Privacy Rights Clearinghouse, said holders of debit cards involved in the Hannaford case are most at risk of fraud. Banks generally cover costs from fraudulent charges on credit cards, but a criminal could potentially drain a victim's bank account and leave them with the task of convincing a bank they deserve to be reimbursed.

"Any time a debit card number is exposed, the affected individuals need to be contacted immediately, and their accounts should be closed down," Givens said.

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

Related Advertising Links

What's This?

The US Dollar Is Falling. Trade It.
Learn to Trade the Dollar. Free GFT Forex Starter...
www.GFTforex.com

US Based Contact Center Solutions
IB/OB, E-Commerce, Fulfillment, IVR, Database...
www.800contactcenter.com

Advertisement

Sprint ahead

The Motorola® i570.

\$69.99
for your business account.

Shop now

E-mail features

What's this?

E-mail newsletters

Sign up to receive our free Tech e-newsletter and get the top news of the day in your inbox.

E-mail



Select one: HTML Text

Breaking news E-mail alerts

Get breaking news in your inbox as it happens

delay in disclosure "puts consumers in a difficult position because they have no way of knowing whether their accounts may have been impacted."

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."

The case ranks among the largest breaches on record involving retailers, but far fewer cards were exposed than in the largest hack. That one began in 2005 — and was disclosed last year — at TJX Cos., the Framingham, Mass.-based operator of more than 2,500 discount retail stores including T.J. Maxx and Marshalls.

TJX reported at least 45.7 million cards were exposed, while banks' court filings put the number at more than 100 million, but there has been no estimate of the total fraud.

Associated Press Business Writer Mark Jewell in Boston contributed to this report.

Copyright 2008 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Share this story:

- Mixx it Digg del.icio.us Newsvine Reddit Facebook What's this?

Posted 19h 38m ago

E-mail | Save | Print | RSS

To report corrections and clarifications, contact Reader Editor Brent Jones. For publication consideration in the newspaper, send comments to letters@usatoday.com. Include name, phone number, city and state for verification.

Conversation guidelines: USA TODAY welcomes your thoughts, stories and information related to this article. Please stay on topic and be respectful of others. Keep the conversation appropriate for interested readers across the map.

You must be logged in to leave a comment. Log in | Register

Empty comment box with a small cursor icon at the bottom right.

Submit

Comments: (6)

Showing: Newest first



bobbylyon wrote: 2h 59m ago Primus and Steelsmith:

Any merchant that accepts or wishes to continue to accept credit cards from the big three - Mastercard, Discover, Visa are required to meet regulations set forth by PCI (Payment Card Industry) Security Standards. Depending on the volume/level of transactions they have to mee a particular tier of security audits that dictate audits and frequency, encryption methods, firewalls, security including authoraization, accountability and access, and policies and practices to protect the customer as well as the organization.

It is way beyond the wireless encryption method they may be using for their store and warehouse operations! This will certainly be an interesting case to watch.

Recommend | Report Abuse



MichaelKinloch wrote: 6h 10m ago

You keep hearing about this stuff each day. They really dropped the ball on this one. Thank goodness for credit protection...like my LifeLock service. I just signed up because they now have WalletLock so they protect your identity and can shut down all your credit cards, etc if fraud happens. FYI...just signed up with a promo code and got the first 30 days free and a discount. The promo code is: jj30.

Recommend | Report Abuse



dwilli11 wrote: 7h 8m ago

WOW!!!! What is up with the local newspapers in the Northeast where Hannaford operates??? They have made no mention of this rip off!!! Could it be because the supermarket is a steady advertising customer??

Recommend | Report Abuse



steelsmith wrote: 7h 49m ago



Somebody fell a sleep at the wheel on this one. It should be mandated that these retailers have the best encryption, securtiy procedures related to credit /debit card transactions. I guarantee that Hannaford was doing what they do bestsetting up systems on the cheap and playing roulette with possibility of doom with their customers being the ones most exposed and in the end paying the price.

Recommend 1 | Report Abuse



primus wrote: 16h 47m ago
I wonder if they were still using the outdated WEP encryption protocols.

Recommend 2 | Report Abuse



phogator wrote: 18h 23m ago
And most of these supermarkets these days want us to give them all of our personal information and swipe a card every time we shop, so they can store information on every purchase we make.

Too many businesses are trying to gather information on us that they don't need, all in the name of "data mining."

Recommend 3 | Report Abuse

Sponsored Links

Radiology Degree Online

Explore degree options in Radiology/X-ray. Free online school info!
www.allaliedhealthschools.com

Forensics Degree Online

Earn Your Degree in Forensics today.
www.education180.com

IronKey Official Site

The world's most secure flash drive w/ advanced encryption technology.
IronKey.com

[Get listed here](#)

Advertisement

Newspaper Home Delivery - Subscribe Today

Home • News • Travel • Money • Sports • Life • Tech • Weather

About USATODAY.com: [Site Map](#) | [FAQ](#) | [Contact Us](#) | [Jobs with Us](#) | [Terms of Service](#)
[Privacy Policy/Your California Privacy Right](#) | [Media Kit](#) | [Media Lounge](#) | [Press Room](#) | [Reprints and Permissions](#)

News Your Way: [Mobile News](#) | [Email News](#) | [Add USATODAY.com RSS feeds](#) | [Podcasts](#) | [Widgets](#)

Partners: [USA WEEKEND](#) | [Sports Weekly](#) | [Education](#) | [Space.com](#)

Copyright 2008 USA TODAY, a division of Gannett Co. Inc.