



Action Alert

March 18, 2008

Hannaford Brothers Supermarkets Hit By Big Data Breach *Are You PCI Compliant?*

Arlington, VA 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 Brothers Inc., grocery chain announced Monday, March 17. 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.

In a statement released Monday March 17, by Hannaford Brothers, maintains that 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 breach is the latest at a big U.S. retailer and comes after U.S. retail group TJX Companies, Inc. disclosed last year that data from 45.7 million credit and debit cards were stolen by hackers over a period of 18 months, as well as personal information for 451,000 people.

HOW DO I PROTECT MY STORE(S)?

There is no full proof manner in which you can protect yourself. However there are mandated requirements that you must do. If you do not do them you are putting your enterprise at severe risk. The most critical compliance for the acceptance of electronic payments is the Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS compliance is now mandated of every merchant that in any way handles, obtains, transmits or stores electronic payment data. Do not be fooled just because your processor is compliant that does not relieve you from having to comply.

N.G.A. wants to make sure you are in compliance. Your company can be with the **N.G.A./CSR PCI Compliance TOOLKIT**, the first and only fully integrated cross-referenced system, which allows the merchant the ability to fully comply with the mandated requirements. The **N.G.A./CSR PCI TOOLKIT** is complete, fully cross-referenced and includes a detailed implementation manual, required self-assessment questionnaire, required procedures, required policies, required training manual, required employee handbook inserts and required penetration or vulnerability scans for one year. The **N.G.A./CSR PCI TOOLKIT** is fully supported by the experience and resources of CSRSI, online, one-on-one email support, and onsite support are available. Your company also receives Breach Insurance upon compliance for one year. The **N.G.A./CSR PCI TOOLKIT** enables level II, III and IV merchants to comply with all the requirements of PCI DSS. CSRSI guarantees that if a merchant completes the **N.G.A./CSR PCI TOOLKIT** and is unable to become PCI Compliant they will receive a full REFUND.

WHAT DO I DO IF IT HAPPENS TO MY STORE?

CSRSI, the creators of The N.G.A./CSR PCI TOOLKIT represents many years of experience and knowledge. The authors of the N.G.A./CSR PCI TOOLKIT have written dozens of papers on the subject and are recognized national experts. According to CSRSI, The best defense is to be well prepared. So here are some suggestions regarding a compromise.

- Immediately put into action your pre-existing containment plan.
- Notify law enforcement.
- Notify your merchant financial institution and/ or processor.

The information that you should have available includes:

- Why you suspect that you have been compromised;
- What documentation you have as to the potential size of the compromise;
- The names of people that have access to the information;
- The name of your processor and merchant bank and the appropriate identifying information;
and
- The physical location and equipment where the suspected breach occurred.

IF BREACH DOES OCCUR AT YOUR LOCATION:

- Contain the exposure.
- Change network and administrator passwords.
- Preserve evidence.

If there is a breach isolate the affected computer from the network by unplugging its cable. Do not turn the affected machine off, log on to it or change any passwords. Change any wireless network passwords, including the router(s). Change all network user and administrator passwords. Preserve the evidence make sure to keep an accurate record of all actions taken, by whom and the time and date of the action.

Visit our website www.nationalgrocers.org for more information on the **N.G.A./CSR PCI Compliance TOOLKIT** or email Mary Wallace at mwallace@nationalgrocers.org or call 703-516-0700.