StoreNext

Update Bulletin

Bank Card Data Breach at Hannaford Bros.

March 20, 2008

Hannaford Bros. announced Monday afternoon that they had suffered a bank card data breach. According to the Associated Press and the many news reports, more than 4.2 million credit and debit card numbers were stolen, resulting in 1,800 cases of fraud to date. Hannaford became aware of the breach on February 27, and investigations indicate that the breach began on December 7. AP reports state that the loss was not fully "contained" until March 10.

The breach reportedly involved all 165 Hannaford Bros. stores in the Northeast, 106 Florida stores in Hannaford's Sweetbay affiliate as well as a small number of Northeast independents that that carry Hannaford products (and that also presumably process payments over Hannaford's network).

Hannaford president and CEO Richard C. Hodge said in a company news release that "The stolen data was limited to credit and debit card numbers and expiration dates and was illegally accessed from our computer systems during transmission of card authorization," implying the theft was from Hannaford's network to the processor for authorization and that card data was not stolen from computer storage media, files or store-level systems.

Since Hannaford uses Retalix StoreLine and WinEPS, customers will likely have questions about the breach and whether they face similar risks. Dealers should feel free to provide the following questions and answers to your customers and prospects.

Did the data breach have anything to do with Retalix's StoreLine point-of-sale software? — No. The data was stolen during transmission from Hannaford's network to the payment processor for authorization.

Was any data stolen from the MTXEPS WinEPS payments software in the stores? — No. As stated by Mr. Hodge, the Hannaford theft was an "…intrusion into its computer network."

Could usable data have been stolen from the WinEPS files in the store? — No. WinEPS is designed to "Payments Application Best Practices" (PABP) and implements the PABP requirement to use strong data encryption in data handling and storage. These encryption algorithms are considered essentially "unbreakable" by current standards, rendering encrypted data from WinEPS useless to data thieves.

Does the Retalix StoreLine POS at these Hannaford and Sweetbay stores meet PCI requirements? — Yes. The PCI compliance rules that apply to POS and WinEPS payments software are called out in PCI's "Payments Application Best Practices" (PABP). StoreLine is compliant with PABP— including the specific versions installed at Hannaford/Sweetbay.

The statement from Hannaford says that the data was accessed "during transmission of card authorization." Is there nothing more specific about exactly how and where this breach occurred? — Facets of the investigation are ongoing, and it is likely that additional information and details will become public.

What data was stolen? — According to CEO Ronald Hodge's statement, "no personal information, such as names or addresses, was accessed or obtained" but the breach did expose customer credit and debit card numbers along with their expiration dates according to Hodge.

On Thursday, Michael Norton, manager of internal communications at Hannaford, said that CVV codes were also taken but reiterated that no Track 1 data was taken.

What's CVV and Track 1 data? — The CVV is an internal code that is an integral part of a card's creation and construction, and it's on Track 2. This is ***not*** the same as the CVV2 code, which is not on any magnetic track – it is printed only on the back of the card. CVV2 is the code used for on-line and card-not-present transactions, not the CVV. Track 1 data includes the card-holder name and sometimes a "member-since" field that can provide information on how long the card-holder has had the account.

What's on Track 2 then? — The full card number, expiration date and the CVV are all on Track 2, and this information is always required by the processor for every transaction. So it is logical that data stolen in the process of transmission would have included all Track 2 data, including these three items. The PIN Block is also on Track 2 if applicable, but the PIN Block is always encrypted in transmission, even though all other Track 2 data must be sent "in the clear."

What steps should ISS45 and ScanMaster users take in general to minimize risk of data breaches? — StoreNext strongly recommends:

- ScanMaster and ISS45 users should ***upgrade to the "isolated" versions*** of these applications, which do not store or handle bank card account numbers, and therefore do not have any bank card account numbers that could be stolen.
- Users should ***complete the PCI self-assessment questionnaire*** (or enterprise audit, if they are classified as a large "Level 1" merchant under PCI). Trustwave, for example, provides on-line services to simplify this task. These assessments are designed to isolate possible security problem areas so that the merchant can resolve them.
- Users need to perform the ***quarterly network scans*** (also required for PCI compliance) to ensure that no unauthorized computers are attached that could be stealing data or installing rogue programs that could enable future thefts. PCI consultants (e.g. Trustwave) are equipped to perform these network scans remotely at a reasonable cost.
- ISS45 and ScanMaster users should implement ***Solidcore*** in the stores. Solidcore provides the strongest anti-virus protection available — especially against the installation of rogue programs that could copy or redirect data on the fly. PCI auditors have also considered Solidcore as providing "compensating controls" that can be used as alternatives to meet the PCI DSS requirements for rolling password changes and immediate installation of operating system updates.
- Users who ***implement Connected Payments*** — instead of in-store WinEPS or other electronic payments software — eliminate the card data storage in store's EPS system by moving it all to the Connected Payments data centers instead. In concert with "isolated" versions of ScanMaster and ISS45, this removes all full bank card number storage from the store, and with it, the possibility of this data being stolen from store locations.

  Connected Payments also implements ***several security features*** up-stream that thwart attacks on data transmissions, including the type that took place at Hannaford.

StoreNext takes very seriously the ongoing task of protecting customer data, and we encourage all grocers to implement the available technology we provide which is specifically designed to reduce or eliminate risks while lowering the cost and effort of meeting the PCI standards.

To Your Success,

Antony van Seventer