

### **TJX Merchant Security Breach communication (posted 1/18/07)**

We have recently been informed by VISA USA of a large-scale compromise involving account data from all card brands. We can now also confirm additional details about the compromise including the name of the retailer and the potential scope of the event.

The compromised retailer is The TJX Companies, Inc. (TJX), a leading off-price apparel and home fashions retailer that operates eight companies and more than 2,300 stores around the world. TJX's store brands include T.J. Maxx, Marshalls, HomeGoods, Bob's Stores and A.J. Wright in the U.S., Winners and HomeSense in Canada, and T.K. Maxx in Europe.

At this point, it appears the breach involves millions of card accounts across all major payment brands accepted by TJX. The affected cards were primarily issued by U.S. financial institutions. While the full extent of resulting fraud from this compromise is not yet clear, patterns of counterfeit fraud have been reported on some of the affected accounts.

If you have any questions about the data compromise, please give us a call.

### **CUNA reports TJX related phishing e-mails (posted 5/9/07)**

A recent phishing e-mail appearing to be from the National Credit Union Administration (NCUA), is targeting consumers' and their fear of security relating to the recent TJX Companies data breach. The false e-mail discusses the TJX Companies data breach, which was made public in January. The breach incidents spanned periods from 2003 through 2006. The phishing e-mail gives the wrong dates for the breach and says VISA notified NCUA in January about the breach.

The notice warns that "magnetic strip information was being stored and your PIN may have been captured" and "strongly" urges NCUA's "members" to update their information within the next 48 hours.

This false e-mail asked for the recipient to click on a link to verify their credit union account registration. If the recipient proceeded to do so, the link directed them to a false website and asked for their credit union account number and PIN, along with other personal information.

Loss Prevention Recommendations:

If you receive an unsolicited e-mail alleging to be from the NCUA, take the following steps:

- Remember that NCUA NEVER asks credit union members for personal account information.
- Anyone who has received a fraudulent phishing e-mail purportedly from NCUA should forward the entire e-mail message to [Phishing@ncua.gov](mailto:Phishing@ncua.gov).

Please see our Loss Prevention Recommendations on the Scar Alerts page of our website.