Emerging Trends in Card Fraud

Protecting Your Financial Institution and Your Cardholders From Fraud

By Heidi Eischens, Fraud Risk Manager, Elan Financial Services

Over the past year, the credit and debit card industries have seen increased fraud activity, and consumers have become more aware of potential threats. Three relatively new fraud trends have stolen headlines around the nation, and financial institutions are preparing comprehensive strategies to fight these emerging card fraud trends.

‘Phishing’ for card information
The first scam has been coined ‘phishing’. Phishing happens when an email is sent reporting to be from a legitimate business, but requests sensitive personal and/or account information such as account numbers, PINs or passwords. Many financial institutions, as well as companies such as eBay, PayPal and BestBuy, have been victims of phishing. Unfortunately, the consumer often believes the business has given the criminals their email information and ultimately blames the business itself for the scam. These emails tend to have misspellings, redundant language and poor English grammar, but they have become more convincing over time.

To guard against phishing, financial institutions should establish and publish information security standards. An industry best practice is to develop an action plan on how to communicate internally and externally if a financial institution should become a phishing victim. While consumers generally will notify a financial institution if they are suspicious, quick action to shut down the fraudulent website and a plan to notify cardholders will minimize the risk to the financial institution’s reputation.

Consumers can gain some protection by installing personal firewalls if they use cable or DSL Internet services and can install anti-virus software to prevent their personal information from ending up on spam lists.

‘Skimming’ card information from the top
Issuers have seen ‘skimming’ over the past 10 years in typical situations where service providers, such as waiters or parking attendants, copied magnetic stripes while they processed legitimate transactions. However in 2003, the industry saw a significant increase in skimming devices installed on ATMs, at service station ‘Pay at the Pumps’ and at merchant point-of-sale terminals. When a card has been skimmed, consumers are unaware that their card data has been copied until they are contacted by their financial institution or until they find fraudulent transactions on their statements.

Merchants and acquirers need to be vigilant at monitoring their equipment and their service providers to thwart the installation of these devices. Sophisticated
skimming at ATMs has included the criminals locating a camera or data capture device on the PIN Pad that allows the PIN to be recorded along with the stripe data. This has led to an increase in counterfeit and cash advance fraud, especially in foreign countries.

‘Hacking’ account data
Another recent scam is related to database compromises involving credit and/or debit card authorization information. These attacks happen when a merchant card processing system or merchant processor is ‘hacked’ or has equipment stolen. Organized criminal groups recruit hackers to tap into and steal the cardholder data for them. Because different hackers use different methods, the method of compromise is continually changing, but the fraud activity patterns remain fairly consistent. Visa® and MasterCard® work closely with law enforcement and pass card numbers suspected of being compromised back to the issuers for action.

Many issuers are monitoring compromises and mitigating fraud losses with detection rules, although occasionally issuers resort to a ‘close and reissue’ strategy. ‘Close and reissue’ should be done only when detection rules have proven ineffective as it is expensive, inconveniences cardholders and causes some to question the fraud protection offered by the issuer.

About the Author
Heidi Eischens holds the position of Fraud Risk Manager, which includes risk analysis and consulting for new projects and initiatives, fraud project management, financial reporting and fraud tool system administration.

Ms. Eischens received her BBA from the University of North Dakota and her MBA from the University of Minnesota.

About Elan Financial Services
With nearly 40 years of expertise, Elan Financial Services is a single source for an array of services that benefit consumers, businesses and your financial institution directly, including ATM, debit card, credit card, merchant programs and more. We recognize your needs and the needs of the industry and offer extensive national network access including the Fastbank® ATM network featuring Fastbank Free, ensuring unrivaled availability and flexibility. Elan is an associate member of the XXX.
U.S. card fraud losses increased slightly over 2002 as consumer usage increased, although issuers and vendors also improved fraud detection tools and processes. Card not present fraud (mail order/telephone/Internet) continues to be problematic but counterfeit has also increased, partly as a result of increased skimming and merchant compromises.

Source: America Bankers Association, BITS Consortium