Volume 6, Issue 6
June 2011

The Learning Kurve

Presented by

Logan katz LLP s.r.l.
Chartered Accountants / Comptables agréés
www.logankatz.com
105-6 Gurdwara Road
Ottawa, ON K2E 8A3
Tel: 613-228-8282
Fax: 613-228-8284
Email: office@logankatz.com

Debit Card Fraud

DID YOU KNOW—Debit card fraud grew by 132% in Canada between 2004 and 2009!

According to RCMP statistics, debit card fraud in Canada grew from $60 million in 2004 to $142 million in 2009. Between 2008 and 2009 alone it grew by 36.2%.

Business use of debit cards is also expected to grow and, as a result, more fraud in business bank accounts and lines of credit will follow, as will identity theft. The cost will be enormous - not just in the actual lost money, but in the lost time and redirected energy of managers to find the source of the loss and determine the cause. Bank accounts will have to be closed and others opened, new cards, new cheques, and new passwords issued. Customers and suppliers using electronic-funds transfer services will have to be notified and other arrangements made for payments. In addition, there will be "insufficient funds" charges on cheques, and automatic withdrawals will be returned to suppliers.

Chip Cards by 2011

As you may have noticed, cards with chips built in for security will be standard in the near future. These chips will be harder for thieves to read than the current magnetic strips, but your business will not be protected if the card is stolen and the PIN discovered. Furthermore, anyone in possession of the card can read the three-digit Card Verification Code (CVC) on the back of the card to make fraudulent online purchases.

How to Protect Yourself

Protecting business from debit card fraud should combine common sense with an awareness of the need for security.

First and Foremost, never give your card and PIN to an employee. Such carelessness is even worse than signing a blank cheque, because it enables the dishonest employee to see the actual amounts in the accounts. No financial institution will reimburse you for stolen funds when you have provided the electronic signature (PIN).

Do not use initials, birth dates, addresses or names as PINs. The PIN and account numbers taken together are supposed to provide a unique identifier as distinctive as your signature. Unfortunately, the PIN is often compromised because the card owners create the number using predictable combinations such as their initials, birth dates, addresses or names of family members or pets. These PINs may be easily cracked if the thief has time to try various combinations from data found in a stolen wallet or purse.

Because using an ATM is so convenient and commonplace, it is easy to forget they still present a security problem both for the institution and for the customer. ATMs can be compromised with substituted card readers and hidden cameras that record each user's key strokes. Such improperly obtained information can be transferred to an illegally made card and used at an ATM within hours.

How to Protect Company Assets

1. Limit your company's exposure by not linking all accounts to the debit card.
2. Reduce the withdrawal limit and the upper credit card limit to avoid large withdrawals or purchases.
3. Change the PIN number on a regular basis. Most financial institutions allow changes over the Internet or at an ATM. Since the communication protocol is extremely secure, the probability of compromise is minimal.
4. Know your account passwords. Many owner/managers leave all online banking responsibilities to a trusted employee. If receipt and pay ment responsibilities are not segregated, even a trusted employee must be monitored regularly. Redirection of funds to phoney suppliers or simple theft could leave your company with sudden and unexpected working capital problems. You can always take legal action against the employee, of course, but what good is that if the employee cannot repay the spent money, and you are in a cash-flow crisis?
5. Attach debit card purchase slips to the original invoice. You can then distinguish between legitimate and fraudulent purchases and withdrawals in the event the debit card is stolen.
6. Retain all transaction slips produced by an ATM or a Point of Sale (POS) terminal. Do not leave them in the ATM, and do not throw them into the trash. The printed balances indicate to the fraudster just how much remains in the account.
7. Use online banking services to review your accounts daily. A good time is Monday morning or after a long weekend, since many frauds are committed when key financial people are away or businesses are closed. If transactions are unusual and cannot be accounted for, contact the financial institution at once.
8. Never respond to email messages claiming to be from your financial institution. As a matter of policy, financial institutions do not ask for account information or any other personal information by email.

Password Security

Most individuals would never consider carrying a PIN in a wallet, purse or briefcase next to a debit card, because the account could be compromised in the event of loss. The increased requirement of passwords for access to accounts for everything from airlines to the Canada Revenue Agency has created a need to record this easily forgettable information in one readily accessible location.

Many business owners use applications such as Outlook to store important information. The ability to co-ordinate cell desktops and laptops with a cell phone or smart phone carried in a briefcase, jacket or purse creates a potential for not only debit card abuse but also identity theft. Owners/managers should be sure that all laptops, desktops and smart devices are secured to avoid unauthorized access. All devices and application software containing sensitive information should be password protected. In addition, all devices should shut down within a limited time when not in use. Since your smart phone may be the very means of notifying a financial institution of a lost or misappropriated debit card or other identification, these gadgets should be carried on your person at all times.

Identity Theft Protection

Many financial institutions now provide a service marketed as identity theft protection. For a fee they will contact all credit card and debit card carriers of a business or individual as soon as they receive notification that a card may have been compromised. Another means of protection is to maintain a list of numbers to call in the event documents are lost or stolen. This information should be stored on a secure online office server or a service provider that can be contacted from a cell phone.

An Ounce of Prevention . . .

Electronic information carried on laptops, smart phones, electronic organizers or on stand-alone office computers provides access to information that, if used by a criminal, can cripple an organization overnight. Careful password protection combined with vigilance when conducting transactions will limit losses to your business.

This'n That at Logan Katz

Logan Katz is a proud sponsor of the Ottawa Art Gallery. We're giving away 5 complimentary OAG membership cards on a first-come, first-served basis. Call Michelle 613-228-8282 ext. 101.

Wishing everyone a safe and enjoyable summer!!