From time to time, card accounts can become compromised. In all cases, the Bank provides the same type of response to suspicious or fraudulent transactions by replacing the card compromised to minimize fraud losses.

As we have seen from recent media stories, hackers are successful in penetrating electronic repositories of credit card information. Typically, the targeted parties are merchants (hotel chains, large retailers, etc. . .) or their merchant acquirers, and even, as was the case a few years ago with Heartland Systems, a large card processor. Sometimes the illegal acquisition of card account information is done on a much smaller scale, often at a single merchant location.

There are fraudsters who used specialized software to generate plausible card account numbers, expiry date and card verification values and attempt to put through multiple authorizations at online merchants. This type of fraud attempt is not unique to Commercial Cards and all Financial Institutions have been targeted. Scotiabank has additional security measures on our processing platform that will prevent these individuals from successfully using card accounts generated in this manner.

**Compromised Accounts**

When the card Networks (Visa, Mastercard and Amex) and/or the credit card issuers become aware that a data compromise has occurred they will attempt to identify all of the card accounts that may have become exposed. They do this by analyzing historical transaction information of every card account number that would have been handled by a particular merchant/acquirer/processor during the time frame of the suspected security breach. Once these accounts have been identified they are placed on a watch list and classified as “Compromised”. When cards are placed on a compromised list, the issuing bank will begin more aggressive monitoring of the card accounts and try to make a determination regarding the probability that these accounts may become abused and will make a decision regarding the re-issue of these accounts. In some cases, it is possible that cards may be re-issued promptly as a preventative measure, while in others, the Bank may elect to wait for hard evidence of fraudulent activity before undertaking the cancellation and re-issue of account numbers.

**Highly Compromised Accounts**

When issuing banks begin to observe active fraud on accounts that are part of a group of accounts that had been classified as compromised, they will usually act promptly to “block and transfer” (i.e. de-activate old account and re-issue a new card) the affected accounts (and sometimes others on the compromised list) to minimize their fraud losses. When this happens, the Bank will notify the program administrators officially that the re-issue process is underway and provide a detailed list of affected cardholders.

Our clients and their cardholders can reduce the risk of fraud by:

**Track Activity via the Internet**

In order to better combat fraud, you and your cardholders should engage in some preventative measures. Credit-based transactions happen in a flash, so clients should not wait for the end of the month to review spending activity.
Fraud Loss Management on Scotiabank Commercial Cards

Your Scotiabank Commercial Card program gives you the tools to control and monitor credit-based spending more often. Statements delivered via the Internet and your web-based reporting capabilities enable you to quickly identify suspicious activity and take corrective action, including contacting the Bank (1-888-823-9657) immediately to dispute the transaction in question.

**Card Protection**

Some additional basic fraud tips for you and your cardholders:

- Sign your card on the signature panel as soon as you receive it.
- Protect your cards as if they were cash; never let them out of your sight.
- Don't leave your Commercial Card in your vehicle. An alarmingly high proportion of all credit card thefts are from motor vehicles.
- Never write down your PIN, memorize it, and never disclose your PIN to anyone.
- Be aware that financial institutions, the police, and merchants should not ask you to disclose your PIN. You are the only person who needs to know it. When selecting a PIN, always avoid the obvious: your name, telephone number, date of birth, or any simple combination thereof.
- Ensure that you get your card back after every purchase.
- Always check sales vouchers for the correct purchase amount before you sign them, and keep copies of your vouchers and ATM receipts. Then, always check your billing statement and verify the amounts of your purchases.
- Don't volunteer any personal information when you use your Commercial Card, other than by displaying personal ID if requested by a merchant. Do not give your account number over the phone unless you initiated the call and you have verified you are dealing with a reputable merchant.
- Quickly report lost or stolen cards
- Install virus protection software on personal computers
- Use caution when using credit cards for online purchases, especially on non-trusted websites
- Keep a record of account numbers, their expiration dates, and the phone number of the Bank's contact centre in a secure place should the need arise to contact us.
- Advise your cardholders to review their monthly card account statements and report any irregularities immediately.
- If you do not recognize or see unauthorized transaction on your Commercial Card statement, please contact Scotiabank immediately at: 1-888-823-9657.

Fraud losses continue to be an important issue not only for Commercial Credit Cards but also for all card products. The creativity and tenacity of fraudsters is a constant that both card issuers and card users have to be keenly aware of and always vigilant to possible attacks.

A multi-front approach involving the Bank, merchants, our clients, as well as the Visa, Mastercard and Amex Networks constitute the best line of defence against possible fraudulent activity. Beyond the program controls and best practices that are available to our clients to help mitigate the risk of fraud being perpetrated on their card accounts, it is important for our clients to understand that Scotiabank operates a very professional Card Security group whose mandate it is to protect both the Bank and its clients from fraudulent card activity.