Interac®
Online

Interac® Online

Protecting your online business from fraud.

Criminals are always looking for new ways to steal funds from unsuspecting customers. As more consumers turn to online merchants to purchase goods and services, criminals are becoming more sophisticated with online fraud, uncovering new ways to deploy deceitful techniques to steal online banking credentials. If successful, they may exploit this stolen information by shopping online using online payment methods, like *Interac* Online, to make fraudulent transactions.

You can make a difference to help reduce online fraud! Our dedicated Fraud Management team has a program in place designed to monitor reported fraudulent activity experienced with the *Interac* Online payment method, and our devoted Fraud Programs team will work directly with merchants experiencing high fraud rates to educate them on, and establish, practices used in the fight against online fraud.

Identifying fraudulent activity

Outlined below are some helpful tips you can use that will assist you in identifying online fraudulent activity. Be sure to look for any of the following:

- Activity that is reported as fraudulent;
  - ~ Be sure to promptly review fraudulent notification emails from the *Interac* Online Fraudulent Activity Information Report mailbox (IOFair@interac.ca), or directly from your Acquirer/ Payment Service Provider;
  - ~ Fraudulent activity notifications will include the unique Primary Account Number (PAN) generated for each *Interac* Online transaction, allowing you to match reported fraud with the original purchase on your system. Where a fraudulent activity notification has been provided prior to shipment of goods or delivery of services, the refund should be processed via the associated PAN. In cases where refunds to the PAN are not possible, we will coordinate the return of funds with your Acquirer/Payment Service Provider;
- Activity that is linked to previously reported fraudulent transactions;
- Activity that is out of expected patterns based on your normal business experience;
- Multiple purchases within a concentrated time period, often for larger than typical amounts;
- Multiple shipments to the same location or region that seem unusual;
- Multiple purchases using the same computer and IP address (or IP range) with different customer credentials;
- Requests to ship goods to P.O. Box addresses (you may wish to restrict shipments to street as opposed to P.O. Box addresses).

Protect your business and brand

Together with participating financial institutions, we are continually updating their online fraud detection systems, but you still can play a critical role in protecting your business and brand. Being alert and carrying out some simple fraud prevention measures will help ensure you're at less risk of encountering online fraud. Here are some of the things you can do to help protect your online business:

- Have a risk management framework in place in order to promote awareness of the risks associated with online fraud;
- If you are suspicious of a transaction, hold the deliveries of goods or services until you are satisfied that the purchase is not fraudulent; and
- If you encounter a fraudulent transaction, forward the transaction details to IOFair@interac.ca and include the *Interac* Online PAN, amount, date, description, and delivery information for goods or services purchased (i.e., name and address details).

For more information about fraud prevention for *Interac* Online contact your Acquirer/Payment Service Provider or dcfprevention@interac.ca.

INT 005-1177 / E