Conducting Your Transactions Online

Federal financial regulators are reporting that Internet threats have changed significantly over the past several years. Sophisticated hacking techniques and growing organized cyber-criminal groups are increasingly targeting financial institutions, compromising security controls, and engaging in online account takeovers and fraudulent electronic funds transfers.

In order to help ensure the security of your online transactions, we want you to know that:

- We will never email, call or otherwise ask you for your user name, password or other electronic banking credentials
- You can help protect yourself by implementing alternative risk control processes like:
  - Making sure you choose an adequate user name and password that, at a minimum, mixes in small case letters, upper case letters and numbers
  - Periodically changing your password (e.g., at least every 90 days)
  - Safeguarding your user name and password information
  - Making sure you have a firewall in place when conducting your financial transactions
  - Logging off the system when you're done conducting business (don't just close the page or "X" out of the system)
  - Monitoring your account activity on a regular basis

In addition, we may require owners of commercial accounts to perform their own risk assessments and controls evaluations. For example:

- Make a list of the risks related to online transactions that your business faces including
  - Passwords being written down and left out in the open
  - The use of old or inadequate passwords
  - The possibility of internal fraud or theft
  - Delays in terminating the rights of former employees
  - The lack of dual control or other checks and balances over individual access to online transaction capabilities
- An evaluation of controls your business uses may include
  - Using password protected software to house passwords in
  - Conducting employee background checks
  - Initiating a policy and process to terminate access for former employees
  - Segregating duties among two or more people so no one person has too much access or control
  - Conducting internal or third party audits of controls
  - Using firewalls to protect from outside intrusion or hackers

Federal regulations provide consumers with some protections for electronic fund transfers. These regulations generally apply to accounts with Internet access. For example, these federal laws establish limits on a consumer's liability for unauthorized electronic fund transfers. They also provide specific steps you need to take to help resolve an error with your account. Note, however, that in order to take advantage of these protections, you must act in a timely manner. Make sure you notify us immediately if you believe your access information has been stolen or compromised. Also, review your account activity and periodic statement and promptly report any errors or unauthorized transactions. See the Electronic Fund Transfer disclosures that were provided at account opening for more information on these types of protections. These disclosures are also available online (or ask us and we will gladly provide you with a copy).

If you become aware of suspicious account activity, you should immediately contact the authorities and contact us at the number listed below.

BANK OF ONTARIO
BRANCH AT GENOA STATE BANK