Financial fraud

RBC
Royal Bank

Contents

Safeguarding your assets against financial fraud

Today you have a wider choice of products, technology and services than ever before, and you have greater flexibility in the way you manage your financial affairs. These choices, however, bring with them a greater need to safeguard against fraud and misuse. We can help.

RBC® believes that working together is the best way to safeguard against financial fraud. We maintain rigorous security procedures to ensure that you can enjoy banking and doing business with RBC in a safe and secure environment.

Outlined in this brochure are a number of everyday safe-computing practices you can use to help prevent the theft and misuse of your personal and financial information.

Keeping your identifiers confidential

Remember to keep your social insurance number (SIN), personal identification number (PIN), passwords, verification questions and answers and secret access codes confidential.

Your social insurance number (SIN)

Your SIN is issued by the federal government and is a piece of personal identification that should always be kept confidential. It is used for the purpose of collecting income-related information and is needed to administer your personal income tax account.

By law you are required to give your SIN to the following people or institutions only:

- Your employer
- The federal government
- Individuals or others preparing tax-related information slips on your behalf (e.g. banks, trust companies, credit unions and investment dealers)

RBC is required by law to ask you for your SIN for income-reporting purposes such as opening registered accounts or reporting income earned on guaranteed investment certificates and investment accounts. If you apply for a loan or mortgage, we will ask you to provide your SIN — providing your SIN for this purpose is optional. We ask for your permission to use your SIN to ensure that we obtain your information, not information about someone with a similar name, from credit reporting agencies.

Never provide your SIN in response to an unsolicited e-mail or phone call. RBC will never ask you for your SIN, either in an e-mail or over the phone, for verification purposes.

Your Client Card, password and PIN

Your RBC Royal Bank® Client Card and PIN (or your Client Card number and password when banking online) give you convenient access to your money around the clock and the world. Your Client Card provides access to a wide range of banking and payment services including banking machines (ATMs), retail (point-of-sale), and RBC Royal Bank Online Banking and Telephone Banking.

Your PIN and password act as your electronic signature to identify you as the authorized user of your Client Card and online accounts. Keep them secret to prevent unauthorized use.

How to choose your PIN

Choose a PIN with numbers and/or letters you can easily remember, but avoid numbers and letters that others might guess. Here are some examples of numbers you should avoid:

- Your birth date
- Your telephone number
- Your address
- Your SIN

When travelling abroad, please keep in mind that many countries around the world accept only four-digit PINs.

How to protect your PIN

Protecting your PIN is among the most effective ways to protect yourself against the scams of unscrupulous people.

- Do not reveal your PIN to anyone including employees of RBC, law enforcement officers, friends and family. Law-abiding individuals will never ask you for it. If you need to ask somebody (e.g. a family member, friend, associate, caregiver) to perform banking activities on your behalf, speak with your banking representative to discuss other options.

- If you suspect that someone knows your PIN, change it immediately at your nearest branch. You can also change your PIN at most RBC Royal Bank ATMs. Contact us immediately if you suspect that someone knows your PIN.
- When conducting a transaction at an ATM or retail (point-of-sale) location, keep your Client Card within sight and shield the keypad while you enter your PIN.

For further information on protecting your PIN, please refer to Interac Association's website at **www.interac.org**, Canada's Office of Consumer Affairs' Debit Card Fraud website at **strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/en/ca01832e.html** or your Client Card Agreement.

Protecting your accounts

Some of your banking transactions may still involve paper transaction documents such as cheques and deposit slips. These documents are often encoded with your account number. Here are some suggestions to help you ensure that your accounts remain confidential and cannot be accessed by unauthorized persons:

- Write cheques using indelible ink (ink that can't be erased), starting at the left-hand margin and leaving no blank spaces.
- If you make an error while filling out a cheque, deposit or withdrawal slip, destroy it (e.g. by tearing it into pieces or shredding it).
- Avoid making cheques payable to "cash" or "bearer" and don't leave the "payee" space blank.
- If a cheque is endorsed (signed on the back by the payee), it can potentially be cashed by anyone. It's a good idea to endorse cheques only when you are ready to cash or deposit them.

- Know when you should receive statements; if the delay seems longer than usual, contact the statement issuer.
- Keep blank cheques, cancelled cheques and account statements in a safe place. Destroy cancelled cheques and account statements when they are no longer needed.
- Check your statements, cheque-imaging copies, cancelled cheques (for business clients) and bankbooks promptly and regularly, and report any discrepancies immediately including missing transactions. You may also want to sign up for Online Banking so that you can regularly monitor and reconcile your accounts. If you notice any discrepancies, report them immediately.
- Request electronic statements.
- Use the online cheque-viewing option to regularly verify the cheques written from or posted to your account. If you notice any discrepancies, report them immediately
- Notify RBC if you are concerned with a cheque that you are cashing or depositing and have received it from someone you don't know or haven't dealt with before.
- Be wary of accepting negotiable items such as personal cheques from unknown persons. Fraudsters often go to great lengths to ensure their counterfeit cheques are high quality, with all the characteristics and attributes of a legitimate cheque. Review items carefully for errors, inconsistencies in font, obvious flaws; and let RBC know right away when you don't know the cheque writer or when you suspect a cheque is a fake.
- Using direct deposit and electronic debit facilities will cut down on the paperwork on your account and may reduce the chance of paper transaction slips falling into the hands of potential fraudsters.

Keeping your Client Card and credit cards safe

Client Cards and credit cards provide convenient methods to conduct your daily transactions. Recognized around the world, they give you broad purchasing power, and in many cases, they allow you to obtain cash and conduct certain transactions at ATMs and retail locations.

Using your Client Card and credit cards with care will help prevent people from using your cards fraudulently. Here are some suggestions:

› Sign your new card as soon as you receive it and call to ensure your credit card is activated immediately. RBC Royal Bank *Visa** cards are activated by calling 1-877-900-5900. Your *Visa* card is automatically linked to your Client Card, which means you are able to make cash withdrawals from your *Visa* using your Client Card even if you haven't yet activated your *Visa* card.

› Cancel any unwanted or expired cards by contacting the card issuer in addition to cutting up the unwanted or expired card. Merely destroying the card will not close the account, so a new card could be issued under the same account number.

› Avoid leaving your card unattended in any public location. Keep your card in view when you use it, and ensure it is returned to you. Look at the name on the card when it is returned to you to ensure it is your card. Destroy receipts that you no longer need.

› Be careful when salespeople swipe your card for you. Make sure you see the card at all times to ensure that they aren't swiping it through another device below the counter. Whenever possible, swipe it yourself.

› Check the sales receipt and purchase amount before you sign the transaction slip.

› Don't forget to retrieve your card from the cashier or ATM after you've completed your transaction(s), and shred or otherwise destroy paperwork you no longer need.

› Never share your Client Card or PIN with anyone, even your friends and family.

› Avoid using your cards or entering a banking machine area if you feel unsafe or crowded.

› If you feel crowded, ask other users to stand back before you enter your PIN.

› When withdrawing cash, verify your cash discreetly and immediately put it in your wallet.

› Regularly check your statement and online banking records to verify all the transactions on your account. Report any discrepancies, including missing transactions, immediately.

› Avoid giving your credit card number on the telephone, unless you initiated the call or have independently verified the phone number and identity of the caller and know they are with a reputable company.

› Photocopy the pieces of identification you carry with you, including your Client Card and credit cards, so you have a record of their numbers in case they are lost. Keep the photocopies in a safe place (such as a safe deposit box) separate from the originals.

› Keep a record of 1-800 numbers so you can call and cancel your Client Card and/or credit cards immediately if necessary.

Lost or stolen cards

If you know or suspect that your RBC Royal Bank Client Card or any of your credit cards are lost or have been stolen, report it immediately at any branch or call our 24/7 telephone line at 1-800-769-2511.

We are working hard to protect you against fraud. If we notice transactions on your card that deviate from your regular banking activity, we may contact you to confirm that you made the transactions in question and that your card hasn't been lost, stolen or used without your consent.

If we telephone you to confirm whether the transactions are yours, you will never be asked to provide any PIN, password, Card Verification Value 2 (CVV2) or SIN information. If you receive a call like this and you are concerned about the identity of the caller, hang up and call 1-800-769-2511. Do not call any number provided to you over the phone or in an e-mail until you have independently confirmed the number.

What am I responsible for?

Your responsibilities as a cardholder are outlined in your cardholder agreements. Take time to review them carefully. Using your Client Card or credit card confirms that you have already read and understood the agreement and agree to its terms and conditions. We also have a 100% security guarantee for online banking at **www.rbcroyalbank.com/online/rbcguarantee.html** and our Guide to Security and Privacy web page at **www.rbcroyalbank.com/online/guidetosecurity.html.**

Electronic transactions

The Internet gives us the ability to conduct business electronically, 24 hours a day, seven days a week. This unprecedented convenience brings with it the need to ensure that confidential financial transactions take place within a secure computing environment. RBC uses the most up-to-date online technology to keep your confidential client information safe and secure. We use internal

authentication procedures to safeguard customer enrolment and password setting. In addition, we are constantly monitoring our online banking and direct investing facilities and security procedures to maintain them at the highest levels of performance.

Many people choose to manage their finances electronically or by telephone using bank services with access codes and passwords. Being careful about how you conduct transactions helps safeguard against unauthorized use of your personal data. When making online or telephone transactions, make sure your computer screen, keypad or telephone display is not visible to anyone when you enter your account number, password, answers to any verification questions and security access codes.

Here are some additional steps you can take to protect your online transactions:

Avoid using public computers

When conducting your financial transactions, avoid using publicly accessible computers (in locations such as libraries and Internet cafés) and computers that are not your own personal or business computers. The computer software used in those other machines might be able to remember user information such as passwords, so you could be leaving confidential information behind.

When using multiple computers, we recommend that you do not use RBC Royal Bank Online Banking or RBC Direct Investing™ Online in a high-traffic environment such as a library or an Internet café. If, however, you must use a highly trafficked computer, remember to sign off and properly close your browser once you've completed your transaction(s). This prevents unauthorized users from accessing your information using the "back" button.

As a further security enhancement, you may wish to enrol in Sign-In Protection, a new Online Banking security feature that offers another level of protection from the potential misuse of your online account. You choose three questions with answers only you would know. Then when you (or an unauthorized user) try to log on from a computer other than your designated preferred computer using your Client Card number and password, you (or the unauthorized user) will be prompted to correctly answer your security questions to gain access. For additional information, visit our website at **www.rbcroyalbank.com/online/guidetosecurity**.

Maintain current antivirus software and a personal firewall

There are numerous resources you can access to protect your home computer and help make your use of the Internet a secure experience. Antivirus software is widely available and can protect you against the newest computer viruses that may damage your computer and your files, but it must be kept up to date to ensure protection against the latest virus threats. As well, by installing and maintaining an up-to-date personal firewall, you can help control the Internet traffic on your computer and block unauthorized visitors. Other controls, such as anti-spyware and anti-spam, will help to protect your computer against unwanted intruders. To find out which tools are important to install and how to test your computer to ensure that these tools are operating properly, visit **www.rbc.com/security**.

Use effective passwords and security questions or confirmations

It may sound like common sense, but choosing a unique password that is both difficult to guess and easy for you to remember is a fundamental element of computer safety. It is also important to change your password regularly. Avoid using the "save password" function on websites; it will save your password to the computer's hard drive where others can pick it up.

Use security features and always remember to log off and close your browser. If you do not ensure your browser is properly closed, information may still be accessible, even after you log off, which could allow someone to access your personal information.

Secure telephone banking

Our telephone banking technology generally uses either Touch-Tone or voice recognition systems to allow you to perform banking transactions over the telephone. Touch-Tone banking requires that you enter numerical information on your telephone keypad. Voice recognition systems enable you to respond to questions verbally over the telephone as well as perform transactions. When using telephone banking, you will need to enter your Client Card number and your password or access code to identify yourself.

Telephone banking safety tips

- Choose a secret access code that's different from your PIN.
- Change your spoken password from time to time.
- Obscure the telephone keypad when entering your password in any location where someone else can view it.
- Avoid situations where your identification information can be overheard if you're providing it verbally.
- Avoid using cellphones for telephone banking — your calls may be intercepted.

Investing with care

Here are some suggestions on how to minimize your potential risk of encountering fraudulent activity when you make investment transactions:

- Only buy from institutions you trust.
- Avoid investments you are uncomfortable with or don't understand.
- Never make investment decisions under pressure.
- Be wary of "get-rich-quick" offers and "hot tips" — you may stand to lose much more than you'll gain.
- Although many investment transactions are conducted by phone or online, be cautious about investment companies without established premises or offices. Scrutinize the investment carefully if you're asked to send money to a post office box, and independently verify the legitimacy of the company.
- Do not respond to unsolicited e-mail about investments, job offers or any requests for personal information without independently verifying the contents of the e-mail or phone call.

REMEMBER — If it looks too good to be true, it probably is!

Keeping your valuables safe

Safeguarding personal property from fraud or theft is a priority for everyone. There are many services designed for this purpose. Here are some examples.

Safe deposit boxes

Safe deposit boxes are a good place to store stocks, bonds, investments certificates, collector coins, important papers and other valuables. It's also a good idea to store photos or videos of jewellery and other valuable household possessions in a safe deposit box for insurance purposes. We suggest you keep an inventory of the contents of your safe deposit box, photocopies of original documents and photographs in a different safe place.

Safekeeping services

When you purchase stocks, bonds or other securities from investment dealers, most firms will offer safekeeping services and assume responsibility for the protection of the securities as long as they remain in the firm's possession. Contact your local branch for more details on this service.

Redeeming securities

Exercise care when cashing in or redeeming securities registered in your name. Once signed, they are considered "fully negotiable" and can be cashed by anyone. Sign them only when you are at the bank or in your broker's office.

About identity theft

Identity theft occurs when someone accesses another individual's personal information (such as their name, date of birth and SIN) and uses it to perform financial activities in that individual's name. This could involve accessing that individual's financial accounts, opening new credit card accounts, charging existing credit card accounts, writing cheques, opening bank accounts or obtaining false loans or mortgages. Often they steal your identity through your SIN, mother's maiden name, date of birth or bank account numbers.

To protect yourself, be aware of some of the methods that can be used to steal your identity. These include stealing a wallet that contains your personal identification information and credit cards, stealing your financial institution statements from mail boxes, diverting mail from its intended recipients by submitting a change of address form, rummaging through your trash or gaining access to your workplace records.

Information transmitted electronically in an insecure environment can also be intercepted.

If you fail to receive your statements, contact your bank immediately.

Recommendations to combat identity theft

- Shred or thoroughly destroy pre-approved credit card applications, bank statements, credit card receipts, bills and related information, and expired and unwanted credit cards when no longer needed.
- Only carry credit cards that you need.
- Sign all credit cards when you receive them.
- Do not carry your SIN card.
- Do not provide personal information such as credit cards, banking cards, PINs, passwords, SIN and date of birth over the telephone unless you initiated the call or can verify that the call is from a legitimate source.
- Do not lend your cards to anyone.
- Immediately report lost or stolen cards.
- Promptly remove mail from your secure mailbox after delivery, and do not leave mail lying around your home or work.
- Avoid mail or telephone solicitations disguised as promotions or surveys offering instant prizes or awards, designed for the purpose of obtaining your personal details including credit card numbers.
- Request a copy of your credit bureau report every year from both Equifax (1-800-456-7166 or 1-514-493-2314 or www.equifax.ca) and TransUnion (1-877-525-3823 or www.tuc.ca).

What to do if your identity is stolen

If you discover unauthorized or missing transactions on any of your accounts, contact your branch immediately or call our 24/7 telephone line at 1-800-769-2511.

Other agencies such as PhoneBusters, Equifax, TransUnion and the Competition Bureau of Industry Canada may be able to assist you if you become aware of possible fraudulent activity, or if you require additional information. You'll find their contact details at the end of this brochure on page 25.

Avoiding common scams

The following are common scams used to gain access to personal and financial data. We have provided suggestions on how to take precautionary measures. Staying informed can help you protect yourself while enjoying the conveniences of today's electronic banking environment.

Skimming

Skimming is the act of obtaining information from a debit or credit card. Most often this data is obtained with a card reader device when the card is used. The PIN is often obtained separately, usually by someone who is watching, hidden cameras or sophisticated devices that may be attached to the machine used. Once the magnetic strip data and PIN are obtained, a counterfeit card is produced and then used. To protect against skimming, always shield the keypad when you enter your PIN at an ATM or point-of-sale terminal. Do not use an ATM that looks like it has been tampered with. Regularly keep track of your account balance and debits, and report any fraudulent activity or missing funds to your branch or 1-800-769-2511 immediately.

Protecting your PIN, password, answers to verification questions and security access codes

Be aware of unauthorized persons claiming to represent your financial institution who ask you to verify or disclose your PIN when your banking card has been lost or stolen. No law-abiding

employee, police officer, financial advisor or lawyer will ever ask you for your PIN. This is confidential information that provides access to the funds in your account.

If you are contacted in this manner, check that all your cards are in your possession. Report any loss immediately (see the contact information at the end of this brochure) and verify that no replacement card has been issued. Even if your cards are in your possession, contact the institution the caller is claiming to be employed with to report the incident.

Fake charities

If you are asked to donate to a charitable cause, don't give your credit card number over the phone or agree to have someone collect a cheque in person. Ask them to mail a pledge form to you or take their telephone number, ostensibly to call them back, if you have reason to believe that the organization is not legitimate. Do not return the phone call until you independently verify that the phone number they gave you is legitimate.

Card switching and shoulder surfing

This is a fraudulent activity that may occur at an ATM. Be aware of anyone who tells you that you've dropped something or offers to help you enter your PIN when having difficulty with the card reader. As you stoop to retrieve it, they may exchange your Client Card for another card. Working together, another person standing nearby will attempt to observe you as you enter your PIN so that both your card and your PIN are in their possession. Check the name on your card before you put it back in your wallet to ensure it is your card. If it is not, report the incident by calling 1-800-769-2511 (available 24/7) and cancel your card immediately. In all cases, always protect your PIN (cover the keypad) when you enter your password. Do not use an ATM that looks like it has been tampered with.

Telemarketing scams

Some telemarketing firms may contact you claiming that you have won a prize, and then ask for your credit card number or request that you purchase a promotional item in order to collect the prize. If you're suspicious that you may be involved in a telemarketing scam, contact PhoneBusters at 1-888-495-8501.

Unusual transaction requests that are "too good to be true"

You may be contacted by phone, mail, e-mail or fax and told that you've won, inherited or been included in a business venture involving large sums of money. If you are selling personal property (e.g. a car or other goods), a fraudulent person may pose as an interested buyer, pay for the goods with a cheque that's substantially greater than the asking price, and then call you to request that you return the overpayment. In many cases, the original cheque used is stolen, counterfeit or altered and is not returned to RBC until a much later date. You won't discover there is a problem with the cheque until you have returned the so-called "overpayment." Be careful about sending any funds back by cheque or wire transfer.

If you are sending a payment via wire, ensure that you are comfortable with your transaction and that you are fully aware of to whom you are sending the funds. If an individual or a third party asks you to make a deposit or open an account on their behalf, ensure you are confident of their identity and the validity of their reasons for the request before you do so. Be extremely wary of this kind of request. You could become an unwitting accomplice to money laundering (handling stolen or unlawfully obtained funds).

Job scams

With so many career resources available on the Internet, searching for opportunities to make extra money, earn money from home or make a career move has never been easier. Unfortunately, not all employment advertisements are legitimate. People should be careful to avoid a recent type of job scam known as a "payment-forwarding scam" or "payment-transfer scam."

Be wary of jobs where they ask you to accept and transfer money from one bank account to another. Often the receiving bank account will be in a different country, and they will request that you have a bank account at a specific bank in Canada. You may be advised to keep a small percentage of the money being transferred as payment.

This type of scam varies and can be quite clever. Fraudsters may request an applicant's bank account information in order to set up a direct-deposit payment schedule, or they may transfer the funds themselves without the applicant's knowledge. Fraudsters may steal company names and corporate logos to make their ad or e-mail invitation more convincing. They may also scan for resumes that job seekers have posted online and then contact them directly. Be aware that if you transfer money that has been stolen or is being laundered, you could be an accomplice to the crime under the law.

Advance-fee scams

Posing as a reputable financial institution by copying its brand and logo, fraudsters promote supposed pre-approved loans and mortgages or unusually high interest rates for investment products. Business is solicited on the strength of the reputation of the financial institution, and money is requested up front to secure the approved credit or high-return investment product.

Phishing and vishing — e-mail or telephone fraud

Phishing is when a fraudster sends an e-mail to alert a recipient to a phony problem with their account that requires their immediate attention. The fraudster will provide a link to a fake website, which mimics a financial institution's website. The recipient is then prompted to input confidential personal information such as their account number and password into the fake system so that the fraudster can capture their information.

Vishing is voice phishing. There are two different vishing approaches:

- Similar to phishing, the fraudster sends an e-mail to alert the recipient to a phony problem with their account that requires their immediate attention. But instead of providing a link to a fake website as in the phishing scam, the e-mail provides a phony customer-support telephone number. When clients call that number, an automated message prompts them to log in by providing account numbers and passwords, using the telephone keypad; the fraudster captures their personal information.
- The fraudster calls a customer directly or leaves a phone message warning the client that their account may be at risk. The impostor then advises the client to call customer support immediately and gives a phony phone number to call. When the client calls that number, an automated message prompts them to log in with their account numbers and passwords using their telephone keypad; the fraudster captures their personal information.

Be careful not to give personal information — especially your account number, card number, PIN, password and verification questions and answers — to people who contact you claiming to represent your financial institution. To ensure

the caller is from a reputable financial institution, verify the phone number of the caller prior to responding to any questions — even if the questions sound legitimate.

Financial abuse

Financial abuse is the misuse of an individual's assets, property or personal information, often by a relative or a person in a position of trust. It can be hard to identify, harder to prove and often extremely hard to accept. It often targets elderly or incapacitated persons and may involve tricking or threatening an individual to provide money, property or personal information to another. This is an offense that could lead to a criminal conviction.

Important contact information

Reporting fraudulent e-mails

Please be aware that RBC will never ask you to provide confidential information through regular e-mail. If you receive an e-mail that asks you to provide confidential information such as your account numbers, PIN or password, do not respond and please notify us by sending an e-mail to information.security@rbc.com. To help us with our investigation, please include a description of the incident and attach any e-mails you received that you suspect may be fraudulent. Avoid changing or retyping any part of the original message as this may interfere with our investigation. Once you have forwarded it to us, please delete the e-mail from your inbox. For more information, visit **www.rbc.com/security/bulletinPhishing.html**.

Issues with RBC accounts and cards

The following are the contact numbers for lost or stolen RBC Royal Bank or Royal Trust Client Cards, chequebooks and account information:

› **Canada and the continental United States**
1-800-769-2511

› **Worldwide (collect calls accepted)**
1-506-864-2275

› **TTY/teletypewriter users only**
1-800-661-1275

› **Lost or stolen RBC Royal Bank *Visa* cards**
1-800-769-2512

If you suspect someone has unauthorized access to any account held with any member of RBC, or that fraud has been committed, call our 24/7 telephone line at 1-800-769-2511.

Important RBC security websites

› **RBC Royal Bank Online Banking security**
www.rbcroyalbank.com/online/online_security.html

› **Consumer information on fraud**
www.rbcroyalbank.com/RBC:RRv-Yo71A8-YAANw@Kpg/products/fraud.html (English)

www.rbcbanqueroyale.com/RBC:RTUfVo-71A8UAAtf6Nxs/produits/fraud.html (French)

› **Information security**
www.rbc.com/security/index.html

› **Making a Complaint or Compliment website**
www.rbc.com/customercare

Fraud victims assistance programs

› **PhoneBusters**
1-888-495-8501
Fax: 1-888-654-9426
E-mail: info@PhoneBusters.com

PhoneBusters puts the information into a secure consumer fraud database and shares it with local, provincial and federal law enforcement agencies. It is set up and endorsed by the Ontario Provincial Police and the RCMP.

› **The Competition Bureau of Industry Canada**
1-800-348-5358
E-mail: compbureau@ic.gc.ca

This is the government agency that investigates fraudulent activity such as telemarketing scams.

› **Equifax**
1-800-465-7166 or 514-493-2314
Website: www.equifax.com

› **TransUnion Canada**
1-877-525-3823
Website: www.tuc.ca

Equifax and TransUnion Canada are the two credit bureaus that have all of your credit history on file.

Other websites of interest

Visit the following websites for more information on fraud and how to protect yourself:

› ***Interac***†
www.interac.org

› **The Canadian Banker's Association**
www.cba.ca/en/issues.asp

› **The Government of Canada's Industry Canada**
www.strategis.ic.gc.ca

› **Industry Canada Consumer Connection**
www.consumer.ic.gc.ca

› **The Financial Consumer Agency of Canada**
Consumer Alerts: www.fcac-acfc.gc.ca/eng/consumers/alerts/default.asp

› **The Office of the Privacy Commissioner of Canada**
www.privcom.gc.ca/aboutUs/message_02_e.asp

Appendix

10 tips for safe computing

1. Protect your personal information. Be aware of current online ploys that try to get you to provide personal and/or financial information. Do not respond to unsolicited e-mails or voice mail that asks for confidential information.

2. Keep your computer healthy. It is very important to check the Web sites of your operating system and Web browser vendors for software "patches" and updates in order to protect against software vulnerabilities.

3. Safeguard your PINs and passwords. Never share your passwords and use ones that are difficult to guess, preferably ones that include a mix of letters and numbers. Change your passwords frequently.

4. Use antivirus software. Antivirus software can protect you from potentially damaging viruses that can enter your computer without your knowledge. You should always use up-to-date antivirus software and one that is capable of scanning files and e-mail messages for viruses.

5. Use personal firewalls. Firewalls create a barrier between your computer and the rest of the Internet. It can help to protect against malicious attacks and block certain types of data from entering your computer.

6. Use anti-spyware. Anti-spyware will help to protect your computer against unwanted software from being installed on your computer without your knowledge. Antispyware also helps protect your computer against pop-up advertising and slow performance.

7. Use anti-spam software. Spam is a growing source of computer viruses. Use up-to-date anti-spam software along with your antivirus software. If you receive spam, remember this: don't try, don't buy and don't reply. Just delete it.

8. Use strong encryption. The stronger the encryption your web browser uses, the more difficult it is for unauthorized individuals to intercept your online activities.

9. Disconnect from the Internet when it's not in use. Disconnecting from the Internet when you are not actively online lessens the chance that someone can access your computer.

10. Remember to log off. Ensure that you always properly log off and close your browser. This will prevent others from being able to view this information later.

To learn more, visit www.rbc.com/security/index.html.

10 tips to safeguard your assets

1. Keep your personal information safe. An identity thief will pick through your garbage or recycling bins, so be sure to shred receipts, copies of credit applications, insurance forms, credit offers received in the mail, etc.

2. Keep personal information confidential. Do not give out personal information on the phone, through e-mail or over the Internet unless you have initiated the contact independently and know the person you're dealing with.

3. Be aware of billing and statement cycles. If your bills or statements don't arrive on time, follow up immediately to ensure they have not fraudulently been redirected.

4. Protect your mail. Get into the habit of clearing your mailbox after every delivery. Make sure that your mail is forwarded or re-routed if you move or change your mailing address.

5. Protect your PIN. Do not reveal your PIN to anyone, including employees of RBC, family members and friends. When conducting a transaction at an ATM or retail (point-of-sale) location, keep you client card within your sight and shield the keypad while you enter your PIN.

6. Limit your risk. Review your daily withdrawal limits on your debit card. If you don't need a high daily limit, reduce it. This will help contain fraud by reducing the amount someone can access.

7. Unusual transactions. Never conduct financial transactions on behalf of strangers.

8. Review your transactions. Regularly review your bank and credit card statements to ensure that all transactions are authorized and any missing transactions are reported. Review your credit report once per year.

9. Limit your exposure. Only carry credit cards in your wallet that you need. It's a good idea to leave your birth certificate and social insurance card at home in a safe place.

10. Contact the authorities. If you suspect you are a victim of fraud or theft, contact the authorities immediately.

This document is also available in French.
Ce document est aussi disponible en français.

For more information on RBC products and services, contact 1-800-769-2511 or visit our website at **www.rbc.com**.

TTY/teletypewriter users only, call 1-800-661-1275. This publication is also available in formats suitable for people who are partially sighted or have limited vision.

VPS21622

07469 (03/2007)