

Financial fraud prevention and privacy protection

Advice from RBC



Contents

PROTECTING YOURSELF FROM FINANCIAL FRAUD	1	PROTECTING YOUR PRIVACY	19
Keeping your identity secure	1	Our commitment to your privacy	19
› Your Social Insurance Number (SIN)	1	Our Privacy Policy and Principles	19
› Personal Identification Numbers and passwords	2	› What information is collected?	19
› How to choose your PIN	2	› How we use your information	20
› How to protect your PIN	3	› Other uses of your personal information	20
Protecting your accounts	3	› Keeping your information safe	20
Card security and protection	5	› Keeping your information accurate	20
› Lost or stolen cards	6	› Your access to information about you	21
What am I responsible for?	7	Information from external sources	21
Electronic transactions	7	› Information about you	21
› Avoid using public computers	8	› Other information	22
› Keep your computer protection software up to date	9	Sharing your information	23
› Choose effective passwords and security questions and confirmations	9	› When authorized by you	23
Secure telephone banking	9	› When required or permitted by law	23
› Safety tips	10	› With RBC companies	23
Investing with care	10	› With RBC employees	23
Keeping your valuables safe	11	› With external service suppliers	24
› Safe deposit boxes	11	Questions, concerns and complaints	24
› Redeeming securities	11	Contact information	25
About identity theft	11	› Reporting fraudulent emails	25
› Recommendations to combat identity theft	12	› RBC phone numbers for banking, credit cards and other account information	25
› Identity theft checklist	13	› Related RBC websites	26
Avoiding common scams	13	› Fraud victims assistance programs	26
› Skimming	13	› Other websites of interest	26
› Fake charities	14	Appendix	
› Card switching and shoulder surfing	14	› Top 10 tips to safeguard your assets	27
› Telemarketing scams	15	› Top 10 tips for safe computing and online privacy	28
› Unusual transaction requests that are “too good to be true”	15		
› Job scams	15		
› Advance-fee scams	16		
› Phishing and vishing: email or telephone fraud	16		
› Ponzi schemes	17		
Financial abuse	18		

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 protect the privacy of your personal, business and financial information. We can help.

Protecting yourself from financial fraud

At RBC®, we believe that working together with our clients 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 safely and securely.

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

Keeping your identity secure

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 collecting income-related information and is needed to administer your personal income taxes.

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

- › Your employer
- › The federal government

- › Financial institutions or other organizations that pay interest on your account(s) and need to prepare tax-related information slips on your behalf (e.g. banks, insurance companies, 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 or insurance products such as universal life insurance. If you apply for a credit product, we will ask you for your SIN; though providing it for this purpose is optional. We ask your permission to use your SIN when we process your application 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 any unsolicited request by email, phone call or website pop-up. RBC will never ask you for your SIN, in an email, a website pop-up or over the phone, for verification purposes.

Personal Identification Numbers (PINs) and passwords

PINs and passwords act as electronic signatures to identify you as the authorized user of your RBC accounts (Client Card, credit card, online banking, telephone banking, etc.). When used in combination with the corresponding card or account number, PINs and passwords provide access to your money and account information, 24 hours a day, from virtually anywhere in the world. You should always protect your PINs and passwords and never disclose them to anyone.

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 accept only four-digit numeric PINs.

How to protect your PIN

Protecting your PIN is one of the most effective ways to protect yourself against scams and fraud. Here are some tips to help you select and protect your PIN:



- › Change your PIN from time to time.
- › Avoid numbers that can be easily guessed or that are tied to your personal information such as date of birth, SIN, address, phone number.
- › Do not write down your PIN or store it electronically.
- › Do not disclose your PIN to anyone, including financial institutions, law enforcement agencies, friends or family. If you need someone (e.g. a family member, friend, associate, caregiver) to perform banking activities on your behalf, speak with your banking representative about options other than sharing your PIN.
- › When conducting a transaction, keep your card within sight and always shield the PIN pad while you enter your PIN.
- › If you suspect that your PIN has been compromised, change it immediately at your nearest RBC Royal Bank® branch.

Protecting your accounts

Some of your banking transactions may still involve paper documents such as cheques and deposit slips, which are often encoded with your account number. Here are suggestions to help ensure 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 by tearing it into pieces or shredding it.
- › Avoid making cheques payable to “cash” or “bearer,” and never 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. A better option may be to go paperless and receive your statements online.
- › Keep blank cheques, cancelled cheques and account statements in a safe place. Securely 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.
- › 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.
- › Be wary of accepting negotiable items such as personal cheques from unknown persons. Fraudsters 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 if you suspect a cheque is a fake.
- › Using direct deposit and electronic debit will cut down on the paperwork on your account and will reduce the physical paper associated with the transactions.

Card security and protection

RBC Client Cards and credit cards provide convenient and secure methods to conduct your daily transactions. Widely accepted, they enable you to obtain cash, make payments and conduct financial transactions at ATMs and retail locations around the world.

Safeguarding your cards and using them with care can go a long way toward helping prevent fraud. Here are a few things you can do:

- › Sign your new card as soon as you receive it, and if applicable, activate it immediately upon receipt.
- › Cancel any unwanted cards by contacting the issuer. Merely destroying a card will not close the account. Destroy all cancelled, expired and previously issued cards.
- › Avoid leaving your card unattended in any public location. Keep your card in view when you use it. Ensure your card is returned to you, and check to make sure your name is on the card. Destroy receipts and statements that you no longer need.
- › Be aware that salespeople may 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 your card or for chip and PIN transactions insert and remove it yourself.
- › Check the sales receipt and purchase amount before you validate the transaction (with a signature or PIN).
- › Never share your cards, PINs or passwords with anyone, even your friends and family.
- › Avoid using your cards or entering an ATM area if you feel unsafe or crowded.
- › If you feel crowded, ask others 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 over the telephone, unless you initiated the call. If you did not initiate the call, independently verify the phone number and identity of the caller as the number on your call display may not be the real number from which they are calling.
- › 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 Customer Support numbers so you can cancel or report issues immediately.

Lost or stolen cards

If you know or suspect that your RBC Client Card or credit card has been lost or stolen, report it immediately by calling 1-800-769-2511 or contacting any branch.

We work 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, and that your card hasn't been lost, stolen or used without your consent. You may be contacted by an agent or through an automated phone call.

We will never ask you to provide any confidential information such as your PIN, password, Card Verification Value 2 (the number on the back of your card) 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 email 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. Use of your cards confirms that you have read and understood the agreement and agree to its terms and conditions.

We also have an RBC Online Banking Security Guarantee. For more information, visit rbccroyalbank.com/online/rbcguarantee and our Guide to Security and Privacy web page at rbccroyalbank.com/online/guidetosecurity.

Electronic transactions

The Internet gives us the ability to conduct business electronically, 24 hours a day, seven days a week. This convenience brings with it the need to ensure that sensitive financial transactions take place securely. RBC uses the most up-to-date online technology to keep your confidential client information safe and secure. We use internal procedures to safeguard customer enrolment and password settings. In addition, we are constantly monitoring our online banking and direct investing sites 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 or security access codes.

To help further secure your Interac[®] Email Money Transfer transactions, ensure you use a question that the recipient can answer but is not easily guessed. Do not include the answer as part of the question.

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

Avoid using public computers

When conducting your financial transactions or other transactions involving your personal information, avoid using publicly accessible computers (such as those found in libraries and Internet cafés) and computers that are not your own personal or business computers. You cannot be sure of the security practices on those computers, and you cannot be certain that there isn't malicious software that might record your personal information such as passwords.

If 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 you must do so, then 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 precaution, we suggest you enrol in Sign-In Protection, an RBC Royal Bank 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 know. Then when you try to log on from a computer other than your designated computer(s), you will be required to correctly answer one of your security questions. An unauthorized user will not know the answers to your security questions and will be denied access. For additional information, visit our website at rbccroyalbank.com/online/guidetosecurity.

Remember also to ensure that you are on private websites. In your browser, look for either the "closed lock" or "unbroken key" icon and for a website address that begins with "https" rather than the "http" you see for public websites (the extra "s" stands for secure).

Keep your computer protection software up to date

Viruses and other malicious programs that are transmitted over the Internet are an ongoing threat to computer systems. Maintain a suite of security software products that includes a reputable personal firewall, anti-virus, anti-spam and anti-spyware, all necessary to provide online protection for your computer and your information. Take advantage of automated software update processes for your web browser, operating system and all software that supports your online behaviour (e.g. browser plug-ins such as PDF viewers) or regularly check the applicable websites for required software patches and updates. To find out which tools are important to install and how to test your computer to help ensure that these tools are operating properly, visit rbc.com/privacyscurity.

Choose effective passwords, security questions and 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.

Some tips for choosing a good password:

- › Use combinations of upper case and lower case letters
- › Use numbers and special characters in your password
- › Ensure your password is at least eight characters long

Sometimes remembering a phrase or a song lyric is an easy way to create a complex password.

Secure telephone banking

Our telephone banking technology uses a Touch-Tone system to allow you to perform banking transactions over the telephone. Touch-

Tone banking requires that you enter numerical information on your telephone keypad. When using telephone banking, you will need to enter your Client Card number and your password or access code to identify yourself.

Safety tips

- › Use your hand or an object to block the telephone keypad when entering your password in any location where someone else could easily view it.
- › Avoid situations where your identification information can be overheard if you're providing it verbally.
- › When using phones for telephone banking, be aware that the “redial” button on some phones will display the last string of numbers entered, which could include what you entered during your telephone banking session. If you are ever concerned about that possibility, simply enter random numbers after you've completed and ended your banking call, and those random numbers will be what is played back on “redial.”

Investing with care

Here are some suggestions on how to minimize your 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. Be especially wary of email SPAM suggesting you urgently buy a new stock.
- › Although many investment transactions are conducted by phone or online, be cautious of 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.

- › Never provide your confidential or financial information in response to unsolicited emails or phone calls.

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 way to protect your valuable documents and small items such as stock certificates, 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.

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, 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 or charging existing ones, writing cheques, opening bank accounts or obtaining false loans or mortgages. With your SIN, mother's maiden name, date of birth or bank account numbers, a thief can steal your identity.

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 through an unsecured environment can also be intercepted. If you fail to receive either your paper or electronic 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 in response to any unsolicited request (including by email, website pop-ups or 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 mailbox after delivery, and do not leave mail lying around your home or work.
- › Do not respond to mail or telephone solicitations disguised as promotions or surveys offering instant prizes or awards that are designed for obtaining your personal details such as your credit card number.
- › Request a copy of your credit bureau file every year from both Equifax (1-800-465-7166 or 1-514-493-2314 or www.equifax.ca) and TransUnion (1-877-525-3823 or www.tuc.ca).

Identity theft checklist

If you have been a victim of identity theft, prompt action may limit the impact on you. Here is a checklist that you can follow if you ever become a victim of identity theft:

- › 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 or 1-800-769-2555 for online services.
- › Contact your creditors; i.e. credit card companies, mortgage companies and other finance companies you may have accounts with.
- › Report it to your local law enforcement.
- › Contact the credit bureaus. For personal identity theft, you should contact the two major credit bureaus: TransUnion and Equifax. Review your current credit bureau to determine if there have been any unauthorized changes.
- › If your mail is missing, contact Canada Post — www.canadapost.ca or 1-800-267-1177.
- › Report the incident to PhoneBusters, Canada's national anti-fraud call centre. PhoneBusters gathers information and intelligence about identity theft and provides advice and assistance to victims — www.phonebusters.com or 1-888-495-8501.

You'll find more contact details on pages 25 and 26.

Avoiding common scams

The following are common scams used to gain access to personal and financial data and our suggestions on precautionary measures you can take. Staying informed can help you to protect yourself.

Skimming

Skimming is the act of obtaining information from the magnetic stripe of a debit or credit card. While chip and PIN technology will help

reduce the instances of skimming for debit and credit cards, it is still possible to skim the magnetic stripe on the cards. Most often the data is obtained with a card reader device when the card is swiped. The PIN is often obtained separately, usually by someone who is watching, hidden cameras or sophisticated devices that may be attached to the machine. Once the magnetic stripe 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.

Fake charities

If you receive an unsolicited call asking you 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 the caller to mail a pledge form to you, or take their telephone number to call them back. Do not return the phone call until you independently verify that the phone number is legitimate.

Card switching and shoulder surfing

While at an ATM, be aware of anyone who tells you that you've dropped something or offers to help you enter your PIN. As you stoop to retrieve a dropped item, they may exchange your card for another. Then, 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. Never let anyone help you enter your PIN or see the numbers you are entering. Before you put your card back in your wallet, check the name to ensure it is your card. If it is not, report the incident immediately by calling 1-800-769-2511 (available 24/7) and cancel your card immediately. Do not use an ATM or point-of-sale device 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, email 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 fraudster 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 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 wiring a payment, make sure you know to whom you are sending the funds. If anyone asks you to make a deposit or open an account on their behalf, ensure you know their identity and are confident that their reasons for the request are valid before you do so, even if you have an emotional connection with them. 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.

Be wary of jobs that ask you to accept and transfer money from one bank account to another. Often the receiving bank account is 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 email 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: email or telephone fraud

Phishing is when a fraudster sends an email to try and trick a recipient into responding with their personal or financial information. Sometimes the email is to alert a recipient to a supposed problem with their account that requires immediate attention. The email will include a link to a fraudulent website, which mimics a financial institution's actual website. The recipient is prompted to input personal information into the phony website, such as their account number and password, which the fraudster captures. Other types of phishing emails can be to inform the recipient of a supposed contest they've won or inheritance they've just received. The point is to get you to input your personal information, which is then stolen by the fraudster for the purpose of committing financial fraud.

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

- › The fraudster sends an email to alert the recipient to a supposed problem with their account. But instead of providing a link to a phony website, the email provides a phony customer-support telephone number. When the client calls that number, an automated message prompts them to log in with their account number and password using the telephone keypad. The fraudster then captures that information.
- › The fraudster calls a client directly or leaves a phone message warning the client that their account may be at risk and to call customer support immediately. However, a phony number is given to the client to call. When the client calls that number, an automated message prompts them to log in with their account number and password, using the telephone keypad. The fraudster then captures that information. They may also ask you for your confidential information such as PINs, credit card number, CVV2 (# on the back of your credit card), date of birth. Do not provide confidential information until you call back a publicly published phone number to verify the legitimacy of the request.

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, independently verify the phone number of the caller prior to responding to any questions, and call the number back, even if the questions sound legitimate.

Ponzi schemes

A Ponzi scheme attracts investors by offering guaranteed and unusually high returns, based on short-term and often complex investments. However, the underlying investments don't exist. Returns are paid to the initial investors from the funds of subsequent investors, rather than from

any actual profit earned. The perpetuation of the scheme requires a continued stream of money from new investors.

Tips to avoid a Ponzi scheme:

- › Beware of claims of guaranteed investments with above average returns.
- › Ensure that you receive detailed written information to fully understand and assess the underlying investment details.
- › Assess the promoter of the investment and do your homework, i.e. background check, are they licensed to sell securities - if they claim they are exempt, check with the local regulator.
- › If you have already invested and you are pressured to reinvest your returns, or there is a disruption of services by the Promotor, contact the local regulator.

Always take the time to thoroughly review and evaluate a plan and the promotor before investing in them.

Financial abuse

Financial abuse is the misuse of an individual's assets, property or personal information, possibly by a relative or a person in a position of trust. Perpetrators of financial abuse often target elderly or incapacitated persons. The abuse may involve tricking or threatening an individual to provide money, property or personal information to another. If you suspect you may have been a victim of financial abuse, contact your branch immediately for assistance.

Protecting your privacy

Our commitment to your privacy

Protecting your privacy and safeguarding your personal and business information is a cornerstone of our business and will always be one of our highest priorities.

RBC companies follow comprehensive privacy policies and security practices in compliance with laws and to support our commitment of trust through integrity in everything we do. Our Privacy Principles describe how we collect and use client information, how and with whom it may be shared and what our security practices and your choices are.

At RBC, we are committed to meeting or exceeding the privacy standards established by federal and provincial legislation and regulatory and industry bodies.

Our Privacy Policy and Principles

Our Privacy Policy is comprised of our Privacy Principles, which apply to all of our dealings with you. The Principles, as described in this brochure, apply to all RBC companies operating in Canada.

The following Privacy Principles reflect our commitment to safeguarding your confidentiality and protecting your personal, financial, health and business information.

What information is collected?

Most of the information we collect is directly from you or the references you provide to us when you apply for products or services, complete a survey or sign up for special offers. We will ask you to provide only the information that enables us to complete your request, to provide better service to you or to offer you the products and services we believe you might be interested in.

How we use your information

We use your personal and financial information for only the purposes communicated to you in your agreement(s) with us. In addition, we will not disclose your personal and financial information to anyone who is not authorized to have it. We will also retain your information only for as long as necessary in order to fulfil the purposes for which we obtained it.

Other uses of your personal information

Under certain circumstances, your personal information may be shared with RBC companies or other third parties to allow us to help you achieve your financial goals. However, if you choose not to have your information shared, we will respect your choice and advise the other RBC companies and third parties of your preference. If you do not wish to receive promotional materials from us or you do not want your personal information shared with other RBC companies, simply visit our website at rbc.com/privacysecurity/ca/your-consent-and-your-choices to make your wishes known.

Keeping your information safe

Protecting your personal, business and financial information and safeguarding you from fraud are among our highest priorities.

In addition to our stringent privacy practices, we employ a diverse range of technologies and security mechanisms to ensure the safety, confidentiality and integrity of your information and transactions. We maintain strict security standards to ensure that your information is protected against unauthorized access, disclosure, inappropriate alteration and misuse.

Keeping your information accurate

We do the utmost to ensure the information we have about you is accurate and complete. We encourage you to help us keep our information about you up to date by contacting us, at any time, to provide us with updates.

Your access to information about you

You may obtain access to the information we hold about you at any time to review its accuracy and have it amended as appropriate. To request access to your information or to ask questions about our privacy policies and how they relate to you, please contact us.

Information from external sources

In addition to the information we collect directly from you and your references, we may also collect financial and other information from credit reporting agencies and other financial institutions. That information is limited to what is needed to provide you with the best possible service.

Information about you

The information we use for fulfilling most financial requests includes:

- › Name and other contact information (for business clients, that includes owners, officers and directors)
- › Social Insurance Number (on account opening)
- › Date of birth
- › RBC account numbers
- › Payment history and creditworthiness

We may use your Social Insurance Number for tax-related purposes if you hold a product generating income and share it with the appropriate government agencies. We may also share it with credit reporting agencies as an aid to identify you.

We may collect information about your health from you or from others, as required and permitted by law, for insurance products and services. Sensitive health information will never, under any circumstances, be shared or used for a purpose other than that of the original intent.

The choice to provide personal or business information is always yours. However, in dealings involving insurance and related financial services, your decision to withhold particular details may limit or prevent us from providing the products or services you have requested. It may also make it more difficult for us to advise you or suggest appropriate alternatives.

We use your information to communicate with you, safeguard your interests and provide the services you have requested. We also use it to keep you abreast of your account activities, authenticate your identity, send you important notices and respond to special needs or inquiries. With your consent, we may also use it to send you information on products and services of potential interest offered by other RBC companies or by our selected third-party suppliers.

Other information

It is our goal to continually improve our service offerings to you. Therefore, we routinely collect non-personal aggregate information from surveys, public archives and websites to help us understand the interests of our clients and to manage our risks.

RBC uses online data collection tools to improve functionality, enhance security, evaluate the effectiveness of our websites and marketing campaigns, and provide visitors with a customized online experience. However, when you visit an RBC website, no information identifying you personally can be collected unless you choose to provide it. You may browse our websites anonymously and privately without revealing any personal or financial information.

Sharing your information

We will only share your information in these cases:

When authorized by you

Credit agencies and other financial institutions routinely contact us for credit and financial information about clients. To comply with these requests, we obtain your consent through the client agreement(s) that you sign when you acquire specific RBC products or services. These agreements outline the conditions and provisions for use of the information.

When required or permitted by law

We are legally required to disclose information related to government tax reporting. As well, in instances such as a legal proceeding or in responding to a court order, we may be required to disclose certain information to authorities. We take strict precautions to ensure that the authorities making the request have legitimate and legal grounds to do so.

We are also legally permitted to disclose personal information in situations such as returning a cheque due to insufficient funds, carrying out legal procedures associated with a delinquent account, in a medical emergency or if there is suspicion of illegal activities.

With RBC companies

To ensure that you benefit from our full range of products and services, and as permitted by law, your information may be shared with other RBC companies. This is done only when the proposed services are available through another RBC company and only with your consent.

With RBC employees

Access to your information is restricted to authorized employees who have a legitimate business purpose for accessing it. For example, when you call us, visit a branch or email us, designated employees will access your information to verify that you are the account holder and to assist you in fulfilling your financial requests.

Unauthorized access to and disclosure of client information by an RBC employee are strictly prohibited. All employees are required to maintain the confidentiality of client information at all times, and failing to do so will result in appropriate disciplinary measures, which may include dismissal.

With external service providers

We may use service providers to perform specialized services such as cheque-printing, research, marketing or data processing. At times, these suppliers may be responsible for processing and handling some of the information we receive from you; however, they are given only the information needed to perform the required service. In addition, we require them to protect the information in a manner that is consistent with our privacy policies and security practices.

In the event a service provider is located in a foreign jurisdiction, they are bound by the laws of the jurisdiction in which they are located and may disclose personal information in accordance with those laws.

Questions, concerns and complaints

If you have any questions about the privacy policies outlined in this brochure or have a concern or complaint about privacy, confidentiality or the information handling practices of RBC companies, our employees or service suppliers, please visit your branch or call us at 1-800-769-2511.

If you are not completely satisfied with our response, please refer to the publication entitled “How to make a complaint,” which provides further recourse. Copies are available at any RBC Royal Bank branch or office and may be acquired by calling 1-800-769-2511 or emailing clientcarecentre@rbc.com. TDD/TTY users should contact 1-800-661-1275 to make their request.

Contact information

Reporting fraudulent emails

Please be aware that RBC companies will never ask you to provide confidential information through regular email. If you receive an email 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 email to information.security@rbc.com.

To help us with our investigation, please include a description of the incident and attach any emails 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 email from your inbox. For more information, visit rbc.com/security/bulletinPhishing.

RBC phone numbers for banking, credit cards and other account information

Banking:

- › Canada and continental United States
1-800-769-2511
- › Worldwide (collect calls accepted)
1-506-864-2275
- › TTY/teletypewriter users only
1-800-661-1275

Credit cards:

- › Canada and continental United States
1-800-769-2512
- › Worldwide (collect calls accepted)
General — 1-416-974-7780
Lost or stolen — 1-514-218-2929
- › TTY/teletypewriter users only
1-800-769-2518

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.

Related RBC websites

- › Privacy & Security
rbc.com/privacysecurity
- › RBC Royal Bank Online Banking
rbcroyalbank.com/online/guidetosecurity
- › Make a Complaint website
rbc.com/customer-care

Fraud victims assistance programs

- › PhoneBusters
1-888-495-8501
1-888-654-9426 (fax)
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
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
www.equifax.com
- › TransUnion Canada
1-877-525-3823
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
- › 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
- › Visa Canada
www.visa.ca
- › MasterCard Canada
www.mastercard.com/ca/gateway/en/index.html

Appendix

Top 10 tips to safeguard your assets

- 1. Keep your personal information safe.** An identity thief will pick through your garbage or recycling, so be sure to shred receipts, copies of credit applications, insurance forms, etc.
- 2. Keep personal information confidential.** Do not give out personal information on the phone, through email or the Internet unless you initiated the contact and know who 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 been fraudulently redirected. Request electronic statements.
- 4. Protect your mail.** Bring in your mail daily. Forward or re-route it if you move, change your mailing address or are away.
- 5. Protect your PIN and passwords.** Do not reveal your PIN or passwords to anyone, including employees of RBC, family and friends. When

conducting a transaction, keep your card within sight and shield the keypad when entering your PIN.

6. **Limit your risk.** Sign all credit cards as soon as you receive them. If they are lost or stolen, report it immediately.
7. **Unusual transactions.** Beware of “too good to be true” or unexpected offers or requests such as, “You’ve inherited a large sum of money. To claim it, send us a deposit first.” Never agree to conduct financial transactions on behalf of strangers.
8. **Review your transactions.** Regularly review your financial statements to ensure that all transactions are authorized, and report any missing or fraudulent ones. Review your credit bureau file annually.
9. **Limit your exposure.** Only carry credit cards you use. Don’t carry your birth certificate and social insurance card when you don’t need them; instead keep them in a safe place.
10. **Contact the authorities.** If you suspect you are a victim of fraud or theft, contact the authorities immediately.

Top 10 tips for safe computing and online privacy

1. **Protect your personal information.** Be aware of schemes that ask for personal or financial information. Do not respond to unsolicited requests for confidential information.
2. **Choose effective passwords.** Choose passwords that are difficult to guess but easy for you to remember. Use multiple passwords, change them frequently and use ones that include a mix of letters and numbers: all essential components of online safety.
3. **Verify a message before you take any other action.** Do not click on a link, call a phone number, wire money or take any requested action, unless you first verify that a request is legitimate. Verify it using information from a source other than from within the message itself.
4. **Limit the online information that you make available about yourself.** Be careful about including personal information online, on social networking sites, in chat rooms and in unencrypted email, as fraudsters may try to get at your information for their own benefit.
5. **Be cautious in your online activity.** Be aware that email scams and malicious websites quickly surface for publicized or recurring events or when any news story breaks. Use caution when accessing new sites.
6. **Be wary of pop-up windows.** Don’t click on any action buttons within a suspect pop-up window, including those requesting financial or identification information and those offering to sell you something.
7. **Maintain a suite of security software products.** This should include a reputable personal firewall, anti-virus, anti-spam and anti-spyware, all necessary to provide online protection for your computer and your information. Beware of pop-up warnings that your computer is infected and instructing you to buy or download software to fix the problem.
8. **Keep your computer healthy.** Take advantage of automated updates for your web browser, operating system and for all software that supports your online behaviour, e.g. browser plug-ins such as PDF viewers, or regularly check the applicable websites for required software patches and updates.

9. Remember to log off. Ensure you properly log off and close your browser to prevent others from being able to view your information later.

10. If it looks too good to be true, it probably is!
Be cautious of emails and websites that promise incredible deals and monetary windfalls. You may end up giving your financial information to fraudsters or downloading malicious software by clicking on a tempting link.

® Registered trademarks of Royal Bank of Canada. RBC and Royal Bank are registered trademarks of Royal Bank of Canada.

™ Trademark of Royal Bank of Canada.

† Registered trademark of Interac Inc. Used under licence.

To learn more, visit rbc.com/privacysecurity

For more information on our products and services, speak to a client services representative or:

- › Visit a branch near you to meet with an advisor

- › Call 1-800 ROYAL® 1-1 (1-800-769-2511)

- › Visit rbc.com

TTY/teletypewriter users can call 1-800-661-1275.
This publication is also available in formats suitable for people who are living with vision loss.

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

