Privacy & Security

Our Canadian Privacy Principles

We are committed to protecting your privacy; and your right to control the collection, use and disclosure of your personal information; whether it is under motusbank's control, or information that has been transferred to a third party for processing, in accordance with Canada's *Personal Information Protection and Electronic Documents Act (2000)*.

- **Accountability**: We have designated a Privacy Officer who is responsible for overall privacy governance and all employees are accountable for compliance to these principles.

- **Identifying Purposes:** Before or at the time we ask you for personal information, we will identify the purposes for which it will be used or disclosed. We may ask for information about your identity, transactions, your application, financial behaviour, or other details particular to the product or service.

- **Consent**: You are always in control of your personal information. We require your knowledge and consent for the collection, use, or disclosure of personal information (except when specific legislative or circumstances apply) and we will explain how your information will be used and with whom it will be shared, in a clear, comprehensive and easy to find manner. We will make it easy to withdraw your consent at any time; however this may affect our ability to provide products and services, or fulfil our commitments to you.

- **Limiting Collection:** We only collect information needed for the purposes we have identified, or the products and services you have requested, and we only collect information by fair and lawful means. This may include (but is not limited to) obtaining personal information about you to establish and verify your identity; better understand your needs; assess your suitability and eligibility for products and services; recommend other products and services; to provide on-going service; detect fraud to both you and the Bank; for collection purposes; or, compliance with legal requirements. We keep this information only for as long as it is needed for the purposes described above, even if you cease to be a member.

  Examples:
  - *When you open an account we need your name and address for identification purposes.*
  - *When you apply for credit-related products, we need information about your financial situation in order to make sound credit-granting decisions, both for you and for us. We require your written consent to obtain credit reports about you. Once we have granted you credit, we are required by the terms of contractual agreements with the credit bureaus to supply regular, current information on the status of loans or credit in order to maintain accuracy, completeness and integrity of information. We do not disclose more than is required, nor for periods longer than required.*
  - *If you open an interest-bearing account or an RRSP or other registered product, by law and for income tax reporting purposes we are required to ask for your Social Insurance Number (SIN).*

  We will ensure our employees are appropriately trained to be able to explain the purposes for which they are collecting your information.

- **Limiting Use, Disclosure and Retention:** Unless you consent otherwise or it is required by law, your personal information will only be used or disclosed for the purposes it was collected. We retain your documentation for the longer of: (a) the duration required to provide products, services or commitments to you; and (b) our legal and regulatory requirements. At the end of this period, we will securely dispose of your personal information.

- **Accuracy**: To ensure we are able to satisfy the purposes for which you have provided your personal information, we will list specific items of personal information to provide our services and do our best to ensure the information we have about you is accurate and complete. As we make decisions based on the information we have, we rely upon you to help us keep your information current.

- **Safeguards**: We will protect your personal information with appropriate physical, technological and organisational safeguards relative to the sensitivity to the information, regardless of the format in which we hold it (physical or electronic) and even when it is being disposed. We regularly train our employees on the importance of maintaining the confidentiality of your information.

- **Openness**: We will make clear, easy to read and consistent information about our policies and practices relating to the management of personal information readily available in writing, by telephone, in publications and on motusbank's website. We will include details of who is accountable for these policies and practices; to whom access requests may be sent; and to whom concerns may be addressed. We will also describe what personal information (if any) is made available to other organisations (including subsidiaries or parents) and why. We will not sell your personal information.

- **Individual Access**: Upon request, we will inform you as to the existence, use, and disclosure of your personal information and be given access to that information. You are entitled to question the accuracy and completeness of the information and have it amended as appropriate. We will endeavour to provide this information to you within 30 calendar days, however occasionally we may need additional time and we will communicate these reasons to you.

- **Challenging Compliance**: You are able to challenge our compliance with the above Privacy Principles. We have simple and easily accessible complaint procedures and we will take appropriate measures to correct information handling practices and policies, where deficiencies are identified. We will notify you of the outcome of investigations..

- **Marketing Preferences:** To manage your marketing preferences, please contact us at 1-833-696-6887, or email the Member Service team below.

For further information on PIPEDA, please visit: https://www.priv.gc.ca/en/privacy-topics/

motusbank Member Service
Tel: 1-833-696-6887
Fax: 1-844-696-6887

concerns@motusbank.ca

You may also contact us by mail or online:

motusbank
Attention: Mario Falvo, Chief Privacy Officer
3280 Bloor Street West
Centre Tower, 7th Floor
Toronto, ON, M8X 2X3

Email us: privacyofficer@motusbank.ca
Online Comment Card: http://www.motusbank.ca/giveusyourfeedback

• Our European Privacy Principles

While motusbank does not have operations in Europe, we are committed to ensuring to full transparency to our members residing in the European Union under the European Union's *General Data Protection Regulation (2017) ('GDPR')*, to ensure they are aware of all of the personal data we handle; specify how we protect their personal data; and provide greater control over how we use their personal information.

For further information on GDPR, please visit: http://www.knowyourprivacyrights.org

motusbank **Member Service**
Tel: 1-833-696-6887
Fax: 1-844-696-6887

concerns@motusbank.ca

You may also contact us by mail or online:

motusbank
Attention: Mario Falvo, Chief Privacy Officer
3280 Bloor Street West

Centre Tower, 7th Floor
Toronto, ON, M8X 2X3

Email us: privacyofficer@motusbank.ca
Online Comment Card: www.motusbank.ca/giveusyourfeedback

• Your Online Privacy

motusbank offers you a variety of ways to bank and interact with us online. Our digital channels offer you control and convenience as well as access to our digital services

Digital banking provides convenient access to information and the ability to perform transactions from home, work or other locations. It is important to be aware that when you communicate via the Internet, other people and software can also communicate with your computer. An inadequately protected computer can be accessed by an unknown party or a virus in a very short period of time.

What we are doing to protect your security

motusbank Online Banking offers you the best security currently available in a commercial environment so that your personal and financial information is protected while in transit between your computer and our server. This is done through the use of industry standard security techniques:

- In addition to encrypted passwords, motusbank's Online Banking services offer enhanced security features, including the use of challenge questions, to help you identify that you are accessing motusbank's Online Banking site (and not a fraudulent site masked to appear as the legitimate online banking site). You will be asked to answer one of your personal challenge questions if you sign in to motusbank's Online Banking or Mobile Banking App from a computer or mobile device that you have not previously registered as 'trusted'.

- Encryption ensures that information cannot be read in transit or changed by scrambling the data using a complex mathematical formula. Some browsers can create a more secure channel than others, owing to the 'strength' of their encryption. motusbank uses the strongest channel available - referred to as 128-bit SSL (Secure Socket Layer). If you have a browser that only supports 'weaker' encryption such as 40-bit or 56-bit SSL, you will need to upgrade your browser before using our site. The longer and more complex the 'key' is, the stronger the encryption. The 40 and 128 refer to the length of the key. Since 128 is longer, than 40, it is more secure.

- Use of robust and multi-layered security of servers and applications, multiple layers of internal and external firewalls which protect motusbank's online environments.

- Regular reviews of our security practices and technology updates as well as regular reviews to ensure our security and privacy policies and standards reflect our industry leading position.

- Access to our databases is strictly managed and systems are in place to ensure security is not breached, including the physical security of our computer hardware and communications.

- Automatic session terminations - To help you protect your information, if there has been no activity for 15 minutes, you will be prompted that your session will be terminated and have the option to continue with your session, if not replied to within five minutes; your online banking session will end automatically.

What you need to do to protect your computer and password

Protecting your password and answers to your secondary challenge questions.

Just as you play a vital role in ensuring the security of your home and your possessions, you too share in the responsibility for ensuring that your personal information is adequately protected. In order for us to ensure that only you are accessing your accounts, we need a unique way of knowing that it's you. Just as the key to your home protects unwanted entry, the online banking 'key' - your password and your secondary challenge questions - ensures that only you can access your accounts.

It is your responsibility to ensure that your 'key' to motusbank Online Banking is protected. Please observe the following security practices:

- Select a password that is easy for you to remember but difficult for others to guess.
- Select your security questions that only you know the answer to.
- Select security image and phrase that is easy to remember and meaningful.
- Do not select a part of your PIN (your ATM 'key') or another password.
- Keep your password and secondary challenge answers confidential - do not share.
- Do not write your password down or store it in a file on your computer.
- Never disclose your password to anyone for any reason. Ensure no one watches you type in your password.
- Change your password regularly. We suggest every 90 days.
- Members are reminded that any password that has been in use prior to March 2012 will be required to follow new requirements the next time their password is reset.

Protecting your computer

- Never leave your computer unattended while using banking services.
- Always exit motusbank Online Banking using the logout button and close your browser if you step away from your computer. Your browser may retain information you entered in the login screen and elsewhere until you exit the browser.
- Prevention of Browser Caching (storing of pages) is enabled by default when using motusbank Online Banking. This prevents secure pages and page information from being stored on your personal computer. It is also a beneficial security feature if you are accessing the site from a shared computer, such as at a friend's house or through a publicly-accessible computer, such as at a library or airport.
- Secure or erase files stored on your computer by your browser so others cannot read them. Most browsers store information in non-protected (unencrypted) files in the browser's cache to improve performance. These files remain there until erased. They can be erased using standard computer utilities or by using your browser feature to "empty" the cache.
- Disable automatic password-save features in the browsers and software you use to access the Internet.
- Install and use a quality anti-virus program. As new viruses are created each and every day, be sure to update your anti-virus program often. It is recommended you update anti-virus definitions automatically. Scan all download files, programs, disks and attachments and only accept files and programs from a trusted source.
- Install and configure a personal firewall on your computer to ensure others cannot access your computer through the Internet.
- Install new security patches as soon as your operating system and Internet browser manufacturers make them available.

Protecting your information when using a public computer

You should be extra vigilant when using publicly available computers. Even if you adopt the tips above to protect your information, you need to bear in mind that even benign programs, like popular desktop search programs, can pose a security risk. Certain programs, such

as Google Desktop, cache items that you have viewed so an unwelcome third party can easily search and find those pages again later. To ensure a safe and secure Internet session, only visit reputable sites. If you visit any questionable web site before motusbank Online Banking, we recommend you close your browser and restart it before proceeding to motusbank Online Banking.

Fraud: Recognize it. Report it. Stop it.

Electronic identity theft can occur when you respond to a fraudulent email that asks for your personal banking information (This is called Phishing). Armed with this information, a person may be able to access your accounts or establish credit, pay for items or borrow money using your name. For this reason, motusbank uses different methods to help you confirm the motusbank Online Banking site is legitimate and secure. These include the selection of a unique personal image, challenge questions and answers and a unique personal code.

Safety precautions for online banking

We will never ask you for your personal passwords, personal information numbers or login information in an email.
If you receive such an email:

- Do not click on any links contained in the email or reply to it;
- Immediately forward the email to security@motusbank.ca
- Delete the email once reported.
- Check the address of any webpages that ask you to enter personal account information. In the toolbar at the top of the page any legitimate banking web site will begin with 'https' to indicate that the page is secure.
- Look for the padlock found in the lower right corner of your screen. If the webpage is legitimate, by clicking on the padlock, you can view the security certificate details for the site. A fraudulent site will not have these details.
- Type in our web address yourself to ensure you are transacting with our server.
- Check your bank and credit card statements regularly to ensure that all transactions are legitimate.

By working together, we can defend potential online information security threats. Contact motusbank at 1-833-696-6887 immediately if you suspect someone has gained knowledge of your password or if you suspect any loss, theft or unauthorized use of your account.

- 100% Security Guarantee

We use world-class encryption security

Security that's the equal of any financial institution in Canada. But the true test is this.

We're so confident in our online security that any unauthorized transactions will be reimbursed completely. **100%. Guaranteed.**

Of course, in order to take advantage of a guarantee like that, you need to do your part as well. Mostly common-sense things, like the following:

- Keep your password and security questions confidential
- Don't store your password and member number together

- Contact motusbank immediately if you've noticed suspicious activity, and make sure that you comply with terms set forth in your account agreements

- Always log out of your Online Banking session and make sure you're using up-to-date anti-virus software

If you take care of those things, we've got your back the rest of the way.

If you'd like more information on agreements, please refer to your Personal Membership Agreement.

• Browser Requirements

Security starts with your web browser

You can protect yourself online by using an up-to-date browser with the most recent security updates. To ensure the security of motusbank Online Banking, we support the following browsers that use 128-bit encryption. Select one of the links below if you need to update your browser to the latest versions of:

Microsoft Internet Explorer

Mozilla Firefox

Apple Safari

Google Chrome

Microsoft Edge

- Supported operating systems include Microsoft Windows and Mac OS X.

- Our website is responsive and accessible on mobile or tablet.

- You should have JavaScript enabled on your browser to use motusbank web properties. We use JavaScript to make our websites easier to use.

- The motusbank Mobile Pay app is supported on the Android platform.

• Email and Text Message Fraud - Phishing

Phishing

Phishing is a scheme that uses fraudulent email, web pages and text messages to gather personal, financial and sensitive information for the purpose of identity theft. Most commonly, users receive spam email (mass email messaging), text messages and pop-up windows that appear to come from legitimate businesses. People have been tricked by these deceptive solicitations into sharing passwords, social insurance, credit card and bank account numbers.

How phishing works

Phishing emails and text messages are sent to many recipients and appear to come from legitimate businesses, sometimes even duplicating legitimate logos and text. Within a phishing email, you may be requested to click on a link that takes you to a fraudulent site or pop-up window where you are asked to submit personal and financial information. A phishing text message may request that you send personal information back to the sender through text message or call a phone number.

In order to increase the chances of a response, messages may imply a sense of urgency or an immediate risk to bank accounts or credit cards if you fail to answer. Special offers and prizes may also be promoted as incentives.

Phishers can access your accounts using your passwords and other information to withdraw money or make purchases. Personal information can also be used by phishers to open new bank or credit card accounts in your name.

Have a concern about email or text message fraud? Email us at: OnlineBankingSecurity@motusbank.ca.

• Debit and Credit Card Fraud

Debit Card Fraud

Debit Card Fraud occurs when the information contained on your debit card is stolen and used to obtain funds from your account without your authorization. Card reading devices are used to obtain the electronic data from the magnetic stripe on your card, and hidden cameras or false PIN pads are used to obtain your personal access code. Please protect your PIN.

How chip technology is different

Chip technology uses an embedded microchip to encrypt information, making it more difficult for unauthorized users to copy or access the data on the card. The move to chip-enabled card technology is the latest innovation in an evolving card payment environment. Chip technology is tested, proven and in wide use around the world, and chip-enabled cards are the new global standard for enhanced safety and security.

Fraud and Debit Card safety

Protecting members from potential losses as a result of financial crime is very important to motusbank. We communicate and work with law enforcement agencies, the INTERAC Association, the Canadian Bankers Association and other financial institutions on an ongoing basis.

• Identity Fraud and Theft

Identity fraud is the stealing of personal information and then using it illegally

If you think you are a victim of identity fraud and are a member, call motusbank immediately at 1-833-696-6887.

Thieves might get documents from your trash, steal your purse or wallet, gather information that you have posted on the Internet, change your address with creditors and apply for new loans or credit cards in your name. You may not be aware of this until months or years have passed.

Protect your personal information: Do not give account or card number information to anyone, whether in person, over the phone or online, unless you are confident to do so. Do not carry your Social Insurance Number card in your wallet unless it is necessary.

Memorize your passwords and bank machine Personal Identification Number (PIN): Don't write down your bank machine Personal Identification Number (PIN) or your online banking password. If you must write these down, keep them in a safe place and do not carry them in your wallet or purse. Never give this information to anyone, even a motusbank employee. Our employees will never ask members for this information, so be suspicious of anyone asking for it

Keep your Personal Verification Question (PVQ) answers confidential: Do not share your Personal Verification Question (PVQ) answers with anyone, and do not disclose them in any emails. Giving your PVQ answers to another person or company places your finances and privacy at risk. motusbank will never request this information.

Report thefts and losses immediately: If your wallet or purse is lost or stolen, call motusbank at 1-833-696-6887 to block your accounts and cards from use. Shred or tear up junk mail and statements: If you don't want mail offers, tear them up or shred them. Identity fraud often occurs by thieves going through trash for this. As well, tear up or shred any personal information such as receipts that show your card numbers or bank statements.

Review your account statements: Report suspicious transactions immediately to motusbank at 1-833-696-6887. Review your credit report: At least once each year, contact a credit bureau to check the accuracy of your credit report.

Protect your Personal Identification Number (PIN): When entering your Personal Identification Number (PIN) at a bank machine or debit terminal, position yourself to block others from observing you enter your PIN. Stay alert.

Practice safe computing: Installing up-to-date antivirus software and firewalls on your computer will help keep your motusbank Online Banking safe.

How to Protect Yourself from Identity Theft: Identity thieves are criminals that will learn and use your personal information to access your financial accounts. Checking your accounts regularly and using the following tips will help keep your banking experience as secure as possible.

Updating anti-virus/spyware software and a firewall on your computer will help keep your motusbank Online Banking safe.

• Other Financial Crime

Cheque Fraud

Cheque fraud is the most common financial crime and account for billions of payments each year, making them a prime target. Counterfeit cheques are not written or authorized by legitimate account holder. Forged cheques are not signed by account holder while an altered cheque has been intercepted and the payee and/or the amount have been altered.

Try to focus on electronic payments such as direct deposit and pre-authorized payments, as it’s harder work for criminals. Keep any cheques in a secure location, as these are common items that thieves will look for during a burglary. Destroy unused cheques right away and review statements as soon as you get them. When laser-printing cheques, use cheque paper with the permanent toner to permanently bond ink.

Moving Money for Strangers

Criminals want you to do their banking. If they earn your trust, they'll use your account to cash phony cheques, collect money from other accounts, and move stolen money offshore. They use a variety of schemes to convince you that they're legitimate. Some will even give you money to earn your trust. By accepting and re-directing electronic deposits (such as wire transfers), you could be participating in a money-laundering scheme if those deposits were proceeds of a fraud or other criminal activity. The stories vary, but the results are the same: fraud and financial loss.

Think about these common criminal activities:

You win the lottery	A criminal tells you you've won a lottery, but taxes need to be paid first. If you're unable to pay the fee on your own, you may be offered financing from someone else (who is involved in the scheme). You receive a cheque to cover the taxes and then wire the money to cover the taxes. Afterward, you learn that the original cheque was fraudulent and that you're responsible for the losses.
Oops, I overpaid	The criminal buys something from you and overpays for the item. After you refund the difference, you learn that the original payment was fraudulent and the charges have been reversed.
Earn money From home	A job offer involves receiving funds into your bank account and then transferring a portion of the collected funds on to another account. After transferring the funds, you learn the original transaction has been reversed.

The man from the 'government' A criminal tells you they are a government official from another country, and that they need your help getting funds out of the country. You receive monies and then forward them. Like the above cases, the original deposit is fraudulent and you're liable for the amount forwarded.

Your phony inheritance A relative you never met has left you money in their will. But you need to pay service fees before receiving the funds. Like the other examples above, this scam can leave you on the hook for significant financial losses.

Minimize the risk

- Never conduct financial transactions on behalf of strangers
- Be wary of any offer that sounds too good to refuse
- Cheques and other deposits can be reversed long after funds have cleared
- Never wire funds until the legitimacy of the cheque or electronic deposit is confirmed
- If you suspect a cheque may be fraudulent, we recommend that you have the cheque certified at the issuing bank (the bank which appears on the cheque)

If you suspect fraud is happening to you, contact motusbank at 1-833-696-6887 immediately.

Beware of Requests to Change a Supplier's Banking and/or Mailing Details

A fraudster may contact a business and say that the supplier's address and banking information have changed. They request that all future payments for this supplier be sent to this new bank account and/or mailing address. This is what it looks like:

- A false fax designed to look like a legitimate fax from the actual supplier
- An email from a fake email account, claiming to originate from the actual supplier
- They call an individual in Accounts Payable with the request, and follow up with a false fax or email, as described above

It is prudent for all businesses to be aware of such scams and consider implementing protective measures. Always make a return call to a trusted contact person at the supplier to validate if this request is legitimate Remember: Do not advise the individual making the request that the validation call will be made; do not use any new telephone number(s) provided by the individual making the request.

Avoiding Internet Stock Fraud

Although the Internet is an excellent tool for investors to easily and inexpensively conduct research on companies of interest, it is also an efficient means of spreading fraudulent investment opportunities and artificially inflating the price of thinly traded securities.

• Enhanced Financial Account Information Reporting

Enhanced Financial Account Information Reporting is a requirement under Canadian law that obligates financial institutions to provide certain information to the Canada Revenue Agency (CRA), to assist in combating tax evasion and in promoting voluntary compliance with tax laws.

- The automatic exchange of financial account information with the United States (U.S.) exists under the Canada-U.S. intergovernmental agreement for the Enhanced Exchange of Financial Account Information with respect to taxes (commonly known as FATCA (reflected in Part XVIII of Canada's Income Tax Act)) signed on February 5, 2014; and

- Canada's automatic exchange of financial account information arrangements with jurisdictions other than the U.S. has been implemented in accordance with the Common Reporting Standard (CRS) (incorporated under Part XIX of Canada's Income Tax Act), effective July 1, 2017.

Further information on these programs is available from:

Canada Revenue Agency

Canadian Bankers' Association

Codes of Conduct and Public Commitments

motusbank is committed to protecting our Members. motusbank is committed to the Code of Conduct for the Credit and Debit Card Industry in Canada.

Compliments & Concerns

motusbank is for members who enjoy doing their banking with people who are dedicated to making your daily banking experience easy, smart and savvy. We're in your neighbourhood to deliver on the difference of local banking. In fact, we're among the leaders of North American banks for customer service. We pride ourselves on delivering genuinely caring, proactive personalized advice and services. We'd like to hear from you. Whether you have a problem you would like addressed, words of praise, encouragement or suggestions on how we can improve, we encourage you to contact us.

Please be sure to provide the name(s) of the staff involved so we can be certain to give proper recognition. Thank you!

By Mail: motusbank
Attention: Member Services
3280 Bloor Street West,
Centre Tower, 7th Floor
Toronto, ON, M8X 2X3

Email: giveusyourfeedback@motusbank.ca
Online Comment Card: http://www.motusbank.ca/giveusyourfeedback