
Safeguarding your financial information

Recent technological advances offering greater convenience, flexibility and opportunity have become part of the foundation upon which the financial system is built. However, an unfortunate consequence of having greater freedom is the risk of identity theft and fraud is also greater.

Since we all depend on this technically sophisticated financial system—and participate in it every day—you may be wondering what we are doing to help ensure cyber security.

Safeguarding the privacy of our clients' personal, business and financial information is a responsibility we diligently uphold. This may come as no surprise. As careful stewards of the wealth entrusted to our care, we are equally committed to—and equally rigorous in—our approach to online data security.

We have rigorous, up-to-date security and technological safeguards to help ensure our clients are well-protected and have access to our services without interruption. Our firm along with RBC follow comprehensive privacy and security practices in compliance with laws and to support our commitment of trust through integrity in everything we do.

In addition to stringent privacy practices, we employ a diverse range of technologies and security procedures to help ensure safety, confidentiality and reliability of information and transactions. This includes using secure socket layer encryption, authentication protocols, firewalls, computer anti-virus protection, data integrity systems and online safety mechanisms.

We also employ a comprehensive security organization, including a security operations center with a global mandate, real-time monitoring, and dedicated incident response capability, backed by extended teams around the world. Our experienced specialists continually monitor for malicious threats and proactively adapt to help ensure we maintain the highest possible privacy and security standards. A dedicated incident response system is also in place to help us respond swiftly and effectively to potential hazards. Beyond our technology and cyber security teams, awareness of the risks associated with identity theft and fraud—as well as training regarding what to do to prevent it—is a top priority for employees at all levels throughout the firm. Indeed, our culture of cyber security expertise helps us actively influence the financial industry through thought leadership, participation on advisory boards and being a founding member of the Canadian Cyber Threat Exchange. We also advise the Canadian government on cyber security policy and strategy.

We will never, under any circumstances, send you an unsolicited email that includes a link or phone number asking you to update or verify your account details or other personal information. To help ensure that your privacy and

information remain confidential, we will use encrypted email when we correspond with you when applicable.

When we receive an email request with instructions for your account, even if it sounds legitimate, we typically will follow up with you directly using the phone number on file to confirm the instructions.

Be assured that we will remain vigilant in our efforts to protect your privacy and safeguard your personal, business and financial information. Additional information regarding RBC's privacy and information security practices, including specific security measures, can be found on our website as indicated below.

We also recommend our clients take precautions to protect themselves. That is why we advise our clients to maintain the security of their systems and adhere to best practices such as installing software updates and being wary of phishing emails and text messages. Please browse the website below for additional steps you can take to help ensure a safer online experience.

RBC privacy and security

www.rbc.com/privacysecurity/us