

If you suspect your account has been breached



Wealth
Management

Act quickly and have a plan. If you believe your accounts have been compromised, follow these steps immediately:

Immediate actions

- **Change all passwords:** Update passwords for your compromised account(s) and any other accounts that share similar credentials
- **Create new accounts if necessary:** For severely compromised accounts, consider closing and reopening with new credentials
- **Secure your device:** Have your computer or mobile device professionally serviced to remove viruses, spyware, malware or other harmful programs
- **Contact financial institutions:** Request safeguards be placed on accounts
- **Freeze your credit:** If your credit information appears compromised, place a freeze on applicable accounts until the matter is resolved
- **Consider credit monitoring:** Sign up for ongoing credit monitoring services (note: some services charge fees)
- **Set up fraud alerts:** Request fraud alerts from credit bureaus to prevent unauthorized account opening

Keep information secure

Identity thieves go to extreme lengths to obtain your personal information. Take action to protect yourself:

Review and monitor your credit

- **Request your credit bureau reports:** Obtain copies from all three bureaus (Equifax, Experian, TransUnion) and review carefully for suspicious activity
- **Check for unauthorized accounts or inquiries:** Look for accounts you didn't open or credit inquiries you didn't authorize
- **Make reviewing an annual habit:** Even without a breach, review reports at least once per year
- **Enable two-factor authentication:** Enroll in two-factor authentication for online accounts if available. Do not share one time passwords (OTP) generated from this process
- **Use strong passwords:** Create passwords of 8–12 characters with a mix of letters, numbers and special characters; change them frequently and never reuse them
- **Store passwords securely:** Use a password manager or secure location; never write them down or share them
- **Encrypt sensitive emails:** Use encryption when sending confidential information by

email; never store sensitive data in email folders

- **Protect your PIN:** Never reveal your PIN to anyone, including RBC Wealth Management employees; shield the keypad at ATMs
- **Control information sharing:** Don't share personal information over the phone or via email unless you initiate contact and know the person. Do not click on links or texts from unknown third parties
- **Minimize what you carry:** Only carry necessary information; leave other documents securely at home
- **Don't overshare:** If disclosing information is optional, decline
- **Destroy sensitive documents:** Shred paper containing personal information

Keep devices secure

Even if you employ strong passwords and carefully destroy sensitive documents, fraudsters could target you via your computer or mobile device. Protect your devices:

- **Update regularly:** Install patches, security updates and new app versions promptly
- **Install anti-virus software:** Protect your device with a reputable anti-virus system

Investment and insurance products offered through RBC Wealth Management are not insured by the FDIC or any other federal government agency, are not deposits or other obligations of, or guaranteed by, a bank or any bank affiliate, and are subject to investment risks, including possible loss of the principal amount invested.

- **Avoid unknown devices:** Never plug in strange or unknown USB sticks or external devices
- **Only install trusted apps:** Don't install apps from unknown or unofficial sources
- **Be cautious on public Wi-Fi:** Avoid accessing financial accounts or sensitive information on public or free Wi-Fi connections
- **Always log out:** Ensure you fully log out of account sessions when finished, especially on shared devices

Stay vigilant

You are the first line of defense in protecting your information and accounts. Continue to monitor your accounts actively:

- **Review account activity regularly:** Become familiar with normal patterns so you can easily spot unusual activity
- **Know best practices of your financial institutions:** For example, RBC Wealth Management will never send unsolicited emails asking you to update or verify account details or personal information by clicking a link or calling a provided phone number
- **Monitor billing and statement cycles:** If statements don't arrive on time, follow up immediately to confirm they haven't been fraudulently redirected

Report and escalate

- **Contact authorities immediately:** If you confirm you're a victim of fraud or identity theft, report it to local law enforcement and the Federal Trade Commission (FTC)
- **Report to the FBI:** File a report with the Internet Crime Complaint Center (IC3) at ic3.gov for cyber-related crimes
- **Notify your bank and financial institutions:** Alert them of the breach so they can monitor for unauthorized activity
- **Document everything:** Keep records of all communications and steps taken

For more information:

- Visit www.rbcwealthmanagement.com/cybersecurity or contact your financial advisor
- Review the RBC Wealth Management Fraud & Scam Recovery Guide: <https://docs.rbcwealthmanagement.com/us/0433-fraud-scam-recovery-guide.pdf>

Having a trusted contact person is important

A trusted contact is like an emergency contact—someone RBC can reach in limited circumstances, such as if your financial advisor has trouble reaching you or has reasonable belief that your account may be exposed to possible fraud.

- **Who to designate:** Choose someone you trust, such as a family member, friend or professional you depend on (accountant, attorney or trustee)
- **What they can and cannot do:** Your trusted contact person will NOT be an authorized party on your accounts, nor will RBC accept instructions from them that affect transactions or change account information in any way
- **Their role:** It's simply another way for RBC to reach you if we need to
- **How to set it up:** Contact your financial advisor with your trusted contact's name, address and phone number