

Scotia Wealth Management[®]

[REDACTED]
[REDACTED]
[REDACTED]

July 20, 2023

Re: Notice of Data Security Incident

[REDACTED]

We are writing to inform you about a situation that involves your personal information.

What Happened?

On June 29, 2023, Scotiitrust received confirmation from a third-party vendor, Ernst & Young LLP (“EY”), that certain of our clients’ information was exposed due to a cybersecurity incident that occurred in May 2023, which compromised an external file transfer system, MOVEit Transfer.

Scotiitrust is the custodian of the investment assets in your account, which are managed by [REDACTED]. [REDACTED] We contracted EY to provide Scotiitrust with routine testing to verify compliance with U.S. government regulations for tax reporting and withholding. Client information was provided to EY to facilitate this testing.

We have been in regular contact with EY to determine the impact to your information and provide any information we can to assist in the investigation.

What Information Was Involved?

EY has informed us that the following information of affiliated individuals may have been exposed: name, date of birth, address, phone number, social security number, driver’s license, and/or passport information.

Investment holdings and account balances were not exposed and Scotiabank systems were not directly compromised in this incident.

Scotia Wealth Management®

What We Are Doing

Out of an abundance of caution, we are offering you complimentary credit monitoring with TransUnion for a period of two years, which will enable you to detect any potentially fraudulent activity appearing on your TransUnion credit report.

What You Can Do to Protect Yourself

We take our obligation to safeguard personal information very seriously and are alerting you about this issue so you can take the following steps to protect your information:

- TransUnion Credit Monitoring: Enclosed within this letter is a TransUnion code that may be used at any time over the next five months to sign up for this complimentary service. It can be activated by following the instructions below.
- Review the Attached Reference Guide. The attached Reference Guide provides additional information on the protection of your personal information, including ordering free credit reports and reviewing recommendations by the U.S. Federal Trade Commission.
- Additional Resources: Please visit the Scotiabank website and select the 'Security and Fraud' tab at the bottom of the page for additional resources on how to protect yourself and your personal information.


For More Information

If you have any further questions or concerns, please call us at 1-877-866-8889 or contact your Relationship Manager.

We sincerely apologize for any concern or inconvenience this may cause.



Scotiabank®
The Bank of Nova Scotia Trust Company
40 King St. West
52nd floor
Toronto, Ontario, Canada
M5H 1H1

Activation Code: 

We have retained the assistance of Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

Through Cyberscout, we have arranged a two-year subscription to an online monitoring service, at no cost to you. This credit monitoring service will notify you by email of critical changes to your Credit Report. Should you receive an email alert, you can review and validate the reported change by logging into the portal. This allows you to identify any potentially fraudulent activity on your Credit Report.

We encourage you to take advantage of this service and help protect your identity. To activate your service, please visit:

<https://secure.identityforce.com/benefit/scotiabank>

You will be prompted to enter the following activation code:

A black rectangular box redacting the activation code.

Please ensure that you redeem your activation code before December 17, 2023 to take advantage of the service.

Upon completion of the enrollment process, you will have access to the following features:

- Access to a credit report with credit score. A credit report is a snapshot of a consumer's financial history and primary tool leveraged for determining credit-related identity theft or fraud.
- Credit monitoring alerts with email notifications to key changes on a consumer's credit file. In today's virtual world, credit alerts are a powerful tool to protect against identity theft, enable quick action against potentially fraudulent activity, and provide overall confidence to potentially impacted consumers.
- Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect consumers against identity theft.

Scotia Wealth Management®

- Identity theft insurance of up to \$1,000,000 in coverage to protect against potential damages related to identity theft and fraud
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Assistance with answering any questions individuals may have about fraud.

Should you have any questions regarding the Cyberscout solution, have difficulty enrolling, or require additional support, please contact Cyberscout at 1-877-694-3367.

Reference Guide

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General and present an incident request report to us about the matter. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Scotia Wealth Management®

Consider Placing a Fraud Alert on Your Credit File.

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax Information Services LLC

P.O. Box 740241

Atlanta, GA 30374

1-800-525-6285

www.equifax.com

Experian Inc.

P.O. Box 9554

Allen, TX 75013 1-888-397-3742

www.experian.com

TransUnion LLC

P.O. Box 2000

Chester, PA 19016

1-800-680-7289

www.transunion.com

Consider Placing a Security Freeze on Your Credit File.

You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

Scotia Wealth Management®

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For New York Residents.

You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
<https://ag.ny.gov/>

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
<https://ag.ny.gov/internet/resource-center>