

KING & SPALDING

King & Spalding LLP
1185 Avenue of the Americas, 34th Floor
New York, NY 10036-4003
Tel: +1 212 556 2100
Fax: +1 212 556 2222
www.kslaw.com

Jarno J. Vanto, Partner
Direct Dial: +1 212 556 2210
Direct Fax: +1 212 556 2222
jvanto@kslaw.com

August 24, 2023

Anthony G. Brown, Maryland Attorney General
Via Idtheft@oag.state.md.us

Re: Notice of Data Breach Affecting Ernst & Young LLP Canada ("EY Canada")

Dear Attorney General Brown,

We write on behalf of EY Canada regarding a security incident involving a third-party service provider.

On May 31, 2023, EY Canada was informed by its third-party supplier, Progress Software, of a security vulnerability involving the supplier's MOVEit Transfer solution. MOVEit Transfer is a file transfer tool used by many organizations, including us, to support the secure transfer of data files.

Upon becoming aware of the issue, EY Canada promptly launched an investigation and took steps to secure its systems. EY Canada has also been working with third-party security experts to investigate the scope of the issue.

Based on the investigation, we believe certain files within the MOVEit tool were compromised, including files that contained personal data of 1 Maryland resident. EY Canada then also undertook an extensive analysis of the affected files to determine which individuals and data may have been affected, and to confirm their identities and contact information. The personal data in the relevant files may have included:

- name, address, taxpayer identification number, tax residency, place and date of birth, cash value, and account balance.

EY Canada is notifying individuals whose personal information may have been accessed and offering them a 24-month complimentary subscription to TransUnion's credit monitoring and identity theft restoration services. EY Canada began mailing notifications on August 24, 2023.

An unaddressed copy of the letter is attached. EY Canada has also established a call center to answer consumers' questions.

EY Canada takes this event seriously, and remains committed to protecting consumers' personal information and assisting those who may have been affected by this incident. By virtue of this notice, EY Law does not waive any rights and reserves all rights under such laws. Please do not hesitate to contact us if you have any questions regarding this letter.

Very truly yours,

s/Jarno Vanto

Enclosure



Attention: Notification Department
100 Adelaide Street West, P.O. Box 1
Toronto Ontario M5H 0B3



August 24, 2023

000001



Dear 

NOTICE OF DATA BREACH

We are writing to notify you of an issue that involves certain elements of your personal data.

What Happened

We are writing to provide you with an update on progress and actions undertaken by a Canadian firm, Ernst & Young LLP ("EY"), to manage the situation affecting our valued client, Sun Life International.

EY provides tax reporting and regulatory filings services for Sun Life International. We notified Sun Life International about an incident relating to a third-party software called MOVEit that is used by EY to support encrypted transfer of files between our firm and our clients. During the incident, hackers unlawfully gained access to and obtained certain files on EY's MOVEit server in Canada. Hundreds of organizations around the world have been affected by the MOVEit vulnerability.

Immediately upon becoming aware of the issue, we launched an investigation and took steps to secure our systems. We have also been working with third-party security experts to investigate the scope of the issue and assist with our response.

What Information Was Involved

Based on our investigation, we believe an unauthorized party gained access to and obtained certain files transferred through the MOVEit tool, including files that may contain your personal data. As a result of the incident, your personal data may have been exposed to others. The impacted personal data varied by individual depending on what was provided for completion of the relevant EY engagement. This may include your name, address, taxpayer Identification number, tax residency, place and date of birth, cash value, and account balance.

Next Steps

We regret any inconvenience this issue may cause you. We are informing you about the issue so you can take steps to protect your personal data from identity theft, phishing and other potential misuse.

What You Can Do

We recommend you remain alert for any unsolicited communications regarding your personal data and review your accounts for suspicious activity. Please also review the "Additional Resources" section included with this letter below. This section describes additional steps you can take to help protect your data, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

Credit monitoring

Through TransUnion, we have arranged a subscription to TransUnion credit monitoring, an online monitoring service, **at no cost to you** for 24 months. This credit monitoring service will notify you by email of critical changes to your TransUnion 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 TransUnion Credit Report.

Please see below for further particulars of the services that will be offered to you as well as instructions on enrolling in these services.

Call centre support

A call centre has been set up to receive calls from affected individuals, in various languages. The call centre can answer frequently asked questions related to the MOVEit incident and, where necessary, escalate follow-up queries to EY for a response. The U.S. call centre will offer support in English from 8:00 am to 8:00 pm Monday through Friday (via 833-596-1092), and 24-hour support Monday through Friday, in English, French and Spanish (via 647-492-4240). Additionally, Cantonese and Mandarin support is available from 9:00 am to 5:00 pm, HKT (via 00 852 5808 9657).



Activation Code: ABCDEF00003

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

Through Cyberscout, we have arranged a **24-month** 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/ernstyoungus>

You will be prompted to enter the following activation code:

ABCDEF00003

Please ensure that you redeem your activation code before 11/30/2023 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.
- ✓ Identity theft insurance of up to \$1,000,000 in coverage to protect against potential damages related to identity theft and fraud¹
- ✓ 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.

¹ Underwritten by certain Underwriters at Lloyd's, under a master group policy issued in the name of Cyberscout Limited, Sontiq Inc. and all subsidiaries for the benefit of program members. Expense reimbursement insurance is only available upon successful enrollment in the online monitoring service. Please see www.sontiq.com/terms-of-use for details.

ADDITIONAL RESOURCES

Order Your Free Credit Report: To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

The three credit bureaus (Equifax, Experian, and TransUnion) provide free annual credit reports only through the website, toll-free number, or request form. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax www.equifax.com	(800) 685-1111
Experian www.experian.com	(888) 397-3742
TransUnion www.transunion.com	(800) 916-8800

Upon receiving your credit report, review it carefully. Errors may be a warning sign of possible identity theft. Here are a few tips of what to look for:

- Look for accounts you did not open.
- Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case.
- Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus 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 credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Federal Trade Commission and State Attorneys General Offices: If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidence of identity theft or fraud, promptly report the matter to your local law enforcement authorities (from whom you can obtain a police report), state Attorney General, and the Federal Trade Commission (FTC). You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

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

For Colorado and Georgia residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

For District of Columbia residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents: The Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.



For New Mexico residents: Consumers have rights pursuant to the Fair Credit Reporting Act (FCRA), such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage consumers to review their rights pursuant to the FCRA by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report:

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Rhode Island residents:

File or Obtain a Police Report: For security incidents generally, you have the right to file or obtain a copy of a police report.

Attorney General: You may obtain information about avoiding identity theft at:
Office of the State of Rhode Island Attorney General
150 South Main Street
Providence, Rhode Island 02903
(401) 274-4400
www.riag.ri.gov

Placing a Security Freeze

You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

You can place, temporarily lift, or permanently remove a security freeze on your credit report online, by phone, or by mail. You will need to provide certain personal information, such as address, date of birth, and Social Security number to request a security freeze and may be provided with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. Information on how to place a security freeze with the credit reporting agencies is also contained in the links below:

<https://www.equifax.com/personal/credit-report-services/>
<https://www.experian.com/freeze/center.html>
<https://www.transunion.com/credit-freeze>

As of June 30, 2023, the reporting agencies allow you to place a credit freeze through the online, physical mail and phone numbers and request that you provide the information listed below. Where possible, please consult the websites listed above for the most up-to-date instructions.

Reporting Agency	Online	Physical Mail	Phone Number
Equifax	Freeze request may be submitted via your myEquifax account, which you can create here: https://my.equifax.com/consumer-registration/UCSC/#/personal-info	Mail the Equifax Freeze Request Form to: Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788 Form may be found here: https://assets.equifax.com/assets/personal/Security_Freeze_Request_Form.pdf	888-298-0045
Experian	Freeze request may be submitted here: https://www.experian.com/ncaconline/freeze	Mail the request to: Experian Security Freeze, P.O. Box 9554, Allen, TX 75013 Request must include: • Full Name • Social security number • Complete address for last 2 years • Date of birth • One copy of a government issued identification card, such as a driver's license, state ID card, etc. • One copy of a utility bill, bank or insurance statement, etc.	888-397-3742
TransUnion	Freeze request may be submitted via your TransUnion account, which you can create here: https://service.transunion.com/dss/orderStep1_form.page?	Mail the request to: TransUnion P.O. Box 160 Woodlyn, PA 19094 Request must include: • Full Name • Social security number • Complete address	888-909-8872

Fees associated with placing, temporarily lifting, or permanently removing a security freeze no longer apply at nationwide consumer reporting agencies.

Placing a Fraud Alert

To protect yourself from possible identity theft, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. You may obtain additional information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or security freeze on your credit report.