



May 23, 2023

Norton Rose Fulbright US LLP
1301 McKinney, Suite 5100
Houston, Texas 77010-3095
United States

Via Email: DOJ-CPB@doj.nh.gov

Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Tel +1 713 651 5151
Fax +1 713 651 5246
nortonrosefulbright.com

Dear Sir or Madam:

I am writing on behalf of my client, Franklin Templeton Investments Corp. ("Franklin Templeton Canada") to provide notice of a security incident.

Franklin Templeton Canada was recently notified that InvestorCOM, a third-party vendor they use to coordinate the delivery of Canadian funds' public disclosure documents, experienced a cybersecurity incident. According to InvestorCOM, a previously undisclosed vulnerability in the managed file transfer service they utilize, GoAnywhere, was exploited to gain access to certain of their customers' data. This GoAnywhere vulnerability impacted many organizations around the world. According to InvestorCOM, the compromise occurred on January 30, 2023, and was discovered by InvestorCOM on March 22, 2023. On April 4, 2023, InvestorCOM provided copies of the Franklin Templeton Canada files involved in this incident. Franklin Templeton Canada immediately activated incident response protocols, opened their own investigation, and began gathering as much information as possible from InvestorCOM. Franklin Templeton Canada conducted a thorough review of the impacted files to determine the nature and extent of any personal information involved and determined that the files involved in this incident included

InvestorCOM has since confirmed that no additional files or Franklin Templeton Canada fund investor information was involved.

Today, Franklin Templeton Canada will begin sending notification letters via First Class Mail to the 5 New Hampshire residents whose personal information was contained in the files involved. This notice is being provided in accordance with N.H. Rev. Stat. § 359-C:19 et seq. Enclosed is a sample copy of the letter.

In response to the incident, and out of an abundance of caution, Franklin Templeton Canada has implemented additional measures to help protect Franklin Templeton Canada account(s), including enhanced protection protocols for heightened due diligence and monitoring. These measures are designed to tighten controls around account access (via both call center and secure web) and transaction and payment processing. Franklin Templeton Canada further notified dealers and investment advisor so that they can consider their account controls as well.

Norton Rose Fulbright US LLP is a limited liability partnership registered under the laws of Texas.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients. Details of each entity, with certain regulatory information, are available at nortonrosefulbright.com.

Page 2

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me.

Respectfully submitted,

Will Daugherty
Partner

Enclosure

May 23, 2023

Dear [CLIENT NAME],

Re: Notice of Third-Party Cybersecurity Breach

Franklin Templeton Investments Corp. (“Franklin Templeton Canada”) takes the protection of our investors’ personal information very seriously. Regrettably, we are writing to advise you of a cybersecurity incident involving a third-party vendor, InvestorCOM, which has potential implications for some of your personal information related to your account(s) with Franklin Templeton Canada as detailed below. **Importantly, given the nature of the services provided by InvestorCOM to Franklin Templeton Canada, Social Insurance Numbers and dates of birth were not provided to InvestorCOM and are not involved in this incident.** In addition, Franklin Templeton Canada’s systems were not affected by this incident and investors’ holdings in Franklin Templeton’s Canadian funds have not been impacted.

The purpose of this letter is to alert you to the incident, advise you of the steps we’ve taken to further protect your Franklin Templeton Canada account(s) since learning of it, and provide information on additional steps you can consider taking to further protect your information.

WHAT HAPPENED

Franklin Templeton Canada was recently notified that InvestorCOM, a third-party vendor we use to coordinate the delivery of our Canadian funds’ public disclosure documents, experienced a cybersecurity incident. According to InvestorCOM, a previously undisclosed vulnerability in the managed file transfer service they utilize, GoAnywhere, was exploited to gain access to certain of their customers’ data. This GoAnywhere vulnerability has impacted many organizations around the world. We understand that the compromise occurred on January 30, 2023, and was discovered by InvestorCOM on March 22, 2023. On April 4, 2023, InvestorCOM provided copies of the Franklin Templeton Canada files involved in this incident. We immediately activated our incident response protocols, opened our own investigation, and began gathering as much information as possible from InvestorCOM.

InvestorCOM has since confirmed that no additional files or Franklin Templeton Canada fund investor information was involved. We have conducted a thorough review of the impacted files to determine the nature and extent of any personal information involved.

WHAT INFORMATION WAS INVOLVED

We have determined that the files involved in this incident included your

As noted above, we do not provide sensitive personal information such as Social Insurance Numbers or dates of birth to InvestorCOM in connection with its services, and therefore such information is not involved in this incident.

WHAT WE ARE DOING

In response to the incident, and out of an abundance of caution, we have implemented additional measures to help protect your Franklin Templeton Canada account(s), including enhanced protection protocols for heightened due diligence and monitoring. These measures are designed to tighten controls around account access (via both call centre and secure web) and transaction

and payment processing. We further notified your dealer and investment advisor so that they can consider their account controls as well.

We have also reported this incident to privacy, securities and financial regulatory authorities and have been advised that InvestorCOM has reported it to law enforcement.

WHAT YOU CAN DO

Although we have implemented additional measures to protect Franklin Templeton Canada accounts, it is always advisable to remain vigilant to the possibility of unauthorized activity in your account(s). If you see anything that looks suspicious, or suspect fraudulent activity on your account(s), call your investment advisor or Franklin Templeton Canada immediately using the contact information below. Also, please see the additional information on steps to help protect your information enclosed with this letter.

FOR MORE INFORMATION

Protecting the privacy of your personal information is important to us, and we regret any inconvenience or concern this incident may cause you. Should you have any questions, you can contact us at _____ between the hours of 8:00 a.m. and 6:00 p.m. EDT, and one of our representatives will be happy to assist you. Thank you for your understanding.

Sincerely,

Ravi Ramaswamy
Senior Vice President
Global Shareholder Services & Privacy Officer

ATTACHMENT A

ADDITIONAL STEPS YOU CAN TAKE

Free Credit Report. Regardless of whether you choose to take advantage of the complimentary identity monitoring, it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Contact information for the three nationwide credit reporting companies is as follows:

<u>Equifax</u>	<u>Experian</u>	<u>TransUnion</u>
<u>Phone: 1-800-685-1111</u>	<u>Phone: 1-888-397-3742</u>	<u>Phone: 1-888-909-8872</u>
<u>P.O. Box 740256</u>	<u>P.O. Box 9554</u>	<u>P.O. Box 105281</u>
<u>Atlanta, Georgia 30348</u>	<u>Allen, Texas 75013</u>	<u>Atlanta, GA 30348-5281</u>
<u>www.equifax.com</u>	<u>www.experian.com</u>	<u>www.transunion.com</u>

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. You may obtain information from the credit reporting agencies and the FTC about security freezes.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, <https://oag.dc.gov>, 202-442-9828.

For Maryland Residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State 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.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400.

For Washington Resident: You may contact the Washington State Office of the Attorney General, 1125 Washington St SE, PO Box 40100, <https://www.atg.wa.gov/consumer->

