2024-225

State Street Corporation
One Congress Street
Boston, MA 02114-2016
statestreet.com

Month DD, YYYY

NOTICE of DATA BREACH

Name
Address
City, State Zip

Dear [Name]:

State Street is a service provider to your retirement plan. We are one of the world's leading providers to institutional investors, including investment servicing, investment management, and investment research and trading. State Street has a longstanding relationship with Fiserv ("Service Provider"), a third- party industry leader, in support of our physical check deposit clearing and processing. On October 16, 2023, our Service Provider notified us that images of some checks they processed for us were compromised in a cyber security breach. We are writing to notify you that copies of checks containing your personal information were impacted.

What Information Was Involved?

The data contained on the check images impacted may have included payee name, address, telephone number, and in some cases, your bank account number and routing number. In limited circumstances, if handwritten information was written on the check manually such as driver's license number, date of birth and/or social security number this information may have also been exposed.

The protection of your information is a matter we take very seriously, and we wanted to inform you of this incident and the steps that you may consider taking to guard against any potential misuse of your information in the future. Your trust and the privacy and protection of your information are our top priorities. We deeply regret any inconvenience and concern this incident may cause you.

What Happened?

Our Service Provider uses an application, MOVEit Transfer, to transmit checks. The application was affected by an industry-wide security breach that was uncovered at the end of May 2023. At that time, a flaw that enabled an unauthenticated user to gain unauthorized access to the MOVEit Transfer database was discovered. Our Service Provider notified State Street on October 16, 2023 that information it processed on our behalf was impacted. Since then, we have been working to review the data to understand the specific impact to State Street and its clients.

What Are We Doing to Protect Your Information?

Upon learning of this incident, we took immediate steps to launch a comprehensive investigation, identify individuals affected and notified regulatory bodies. To help prevent something like this happening again, our Service Provider has remediated all technical vulnerabilities and applied patches to the MOVEit Transfer application in accordance with the MOVEit software provider's guidelines. Our Service Provider also mobilized a technical response team to examine the relevant MOVEit Transfer systems and to prevent any further vulnerabilities.

We have arranged for you to receive a two-year complimentary identity monitoring service through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include credit monitoring, fraud consultation, and identity theft restoration. For more information on how to activate your identity monitoring, please review Attachment A that follows this letter. For questions relating to this service, you may contact Kroll at (866) 731-2256.

Steps You Can Take/What You Can Do

We encourage you to remain vigilant for incidents of fraud and identity theft by regularly reviewing account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission (FTC) or law enforcement to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the FTC at:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
https://www.identitytheft.gov/

If you find that your information has been misused, the FTC encourages you to file a complaint with the FTC and to take the following additional steps: (1) close the accounts that you have confirmed or believe have been tampered with or opened fraudulently and (2) file and keep a copy of a local police report as evidence of the identity theft crime. You should also report incidents of suspected identity theft to the state attorney general.

Obtain Your Credit Report

We also encourage you to monitor your credit reports. You may periodically obtain credit reports from each nationwide credit reporting agency. If you discover inaccurate information or a fraudulent transaction on your credit report, you should request that the credit reporting agency delete that information from your credit report file. The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC's "Summary of Your Rights Under The Fair Credit Reporting Act" provides an overview of your rights under FCRA and is available online at https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or by contacting the FTC using the information provided above.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major credit reporting bureaus to request a copy of your credit report.

Place a Fraud Alert or Security Freeze on Your Credit Report File

In addition, you may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to

obtain credit. If you suspect you may be a victim of identity theft, you may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed below. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. An initial fraud alert will last 90 days.

Also, you can contact the nationwide credit reporting agencies regarding if and how you may place a security freeze on your credit report to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization. To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail

However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. The credit reporting agencies have three (3) business days after receiving a request to place a security freeze on a consumer's credit report. There will be no charge for a security freeze.. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

More Information

Again, we apologize for any inconvenience caused by this incident. If you have any questions regarding this incident, please call (866) 731-2256, Monday through Friday between 8:00 am and 5:30 pm CT or if you desire further information or assistance, including information about what data we maintain about you, please do not hesitate to contact State Street directly at dataincident@statestreet.com.

Sincerely,
STATE STREET BANK AND TRUST COMPANY

State Contacts

IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT:

You may contact the DC Attorney General at:

Office of the Attorney General
441 4th Street NW
Washington, DC 20001
(202) 727-3400
https:// oag.dc.gov/

IF YOU ARE AN IOWA RESIDENT:

You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at:

Office of the Attorney General
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5926
www.iowaattorneygeneral.gov

IF YOU ARE A MARYLAND RESIDENT:

You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(410) 576-6491
www.oag.state.md.us

IF YOU ARE A MASSACHUSETTS RESIDENT:

You have the right to obtain any police report filed in connection to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

IF YOU ARE A NEW YORK RESIDENT:

You may contact:
The New York Department of State
Division of Consumer Protection
One Commerce Plaza,
99 Washington Avenue
Albany, NY 12231-001
(518) 474-8583/ (800) 697-1220
http://www.dos.ny.gov/consumerprotection/

IF YOU ARE A NORTH CAROLINA RESIDENT:

You may obtain information about preventing identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.gov

IF YOU ARE AN OREGON RESIDENT:

You may obtain information about preventing identity theft from the Oregon Attorney General. You should also report incidents of suspected identity theft to this office, along with local law enforcement and the FTC. The Oregon Attorney General can be reached at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096

(503) 378-4400
http://www.doj.state.or.us/

IF YOU ARE A RHODE ISLAND RESIDENT:

You may obtain information about preventing identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903 (401) 274-4400
http://www.riag.ri.gov/

ATTACHMENT A

Credit Monitoring Detail (separate file)