

**VIA CERTIFIED U.S. MAIL**

August 30, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Dear Sir/Madam:

I write to you on behalf of Leader Bank, N.A. ("Leader Bank") whose corporate offices are located at 180 Massachusetts Avenue, Arlington, Massachusetts, 02474, to notify you of a data security incident with respect to a third-party vendor of Leader Bank involving the nonpublic personal information of five (5) Maryland residents, pursuant to MD Comm. Law Code § 14-3504. As noted below, Leader Bank reserves the right to supplement this notice with any significant details learned subsequent to this submission. By providing this notice, Leader Bank does not waive any rights or defenses regarding the applicability of Maryland law (including MD Comm. Law Code § 14-3504), the applicability of any other laws of this or any other state, or the existence of personal jurisdiction over Leader Bank.

NATURE OF THE DATA SECURITY INCIDENT

On August 3, 2023, Leader Bank received a notice from its third-party vendor providing core banking services (specifically deposit operations, loan servicing and online banking) of a data security incident relating to the MOVEit software vulnerability. This zero-day vulnerability, as announced by Progress Software on May 31, 2023, allowed malicious actors to access files that were intended to be transmitted securely using MOVEit. Specifically, Leader Bank's vendor disclosed that it used MOVEit to transfer certain files containing data of Leader Bank clients, and the vendor's MOVEit Transfer platform had accessed by an apparently malicious actor between May 27 and May 31, 2023, allowing for the exfiltration of those files. The vendor further advised that they had not determined that Leader Bank data had been accessed until shortly prior to the August 3 notification.

Leader Bank immediately began its own investigation and review of the impacted files and determined that unencrypted client names together with one or more account numbers for said clients were contained in the files accessed due to this vulnerability. According to the written explanation provided by Leader Bank's vendor, no other server containing Leader Bank client data was impacted by this vulnerability and the vendor has not identified any other files that contained unencrypted identifiable nonpublic personal information that was exposed in this incident.

NUMBER OF MARYLAND RESIDENTS AFFECTED

Based on the information in the files provided as cross-referenced with Leader Bank's own databases, the names and account numbers of five (5) Maryland residents were exposed in this incident. Simultaneously with this letter, on August 30, 2023 Leader Bank has sent notices to all impacted Maryland residents by United States mail. A sample copy of the notice provided is attached hereto.

STEPS TAKEN OR STEPS THAT WILL BE TAKEN RELATING TO THE INCIDENT

Safeguarding our clients' personal information is of the utmost importance to Leader Bank. We immediately conducted our own review of the files impacted and have engaged in follow up conversations with the vendor to ensure that the impacted systems have been fully remediated and that appropriate security enhancements have been made, requiring documentation of these steps in writing. We further understand that the vendor is working closely with law enforcement authorities on this matter and has advised the Department of Treasury of this instance given their work in the banking financial system.

With respect to our own processes, Leader Bank implemented its own enhanced monitoring protocols with respect to all affected accounts which could be at risk for fraudulent debits (transactional deposit accounts and lines of credit) and are in the process of hiring additional personnel to allow for more detailed fraud and transaction monitoring. The Bank also will be engaging a dark web monitoring service to determine if these files are available or published in the future and will work with all affected clients to review affected accounts, set up alerts for transactions, or open new account numbers if the client so desires. As part of this notification, all affected individuals have been provided with two (2) years of free identity theft protection services as offered by Kroll.

To date, Leader Bank has not detected any instance of fraud on any affected account arising from this incident and will continue to monitor on a going forward basis. Our vendor has indicated that their investigation remains ongoing, and although the Bank believes it has reviewed thoroughly all affected files and believes the scope of this notification is complete, in the event additional information is made available that impacts Maryland residents, we will ensure that your office is updated as soon as possible. If you require any further information or have any questions regarding the incident described herein, please do not hesitate to contact me by telephone at 781-641-7550 or bames@leaderbank.com.

Sincerely,



Brook Ames
SVP, General Counsel & Chief Risk Officer
Leader Bank, N.A.

Enclosure

cc: Colm Kennedy, VP & Chief Information Security Officer, Leader Bank, N.A.



August 30, 2023

[Name]

[Address]

[City, State, Zip]

NOTICE OF DATA SECURITY INCIDENT

Dear [Name],

We are writing to notify you about a recent cyber vulnerability which has impacted hundreds of companies around the country and the world, including one of our vendors who provides services to many banks across the country. We are sending you this letter to provide you details about what happened, the measures taken in response, and to provide you with information on steps you may want to take to help protect your personal information.

What Happened?

On August 3, 2023, our vendor notified us of an incident related to vulnerabilities discovered in MOVEit Transfer by Progress Software, the commonly used secure Managed File Transfer (MFT) software supporting file transfer activities by thousands of organizations around the world. Our vendor has advised us that they utilized the MOVEit Transfer software as part of their support of Leader Bank's services.

Analysis to date has identified unauthorized activity in the relevant MOVEit Transfer environment between May 27 to 31, 2023, which was before Progress Software publicly disclosed the existence of this vulnerability on May 31. During that time, unauthorized actors obtained files transferred via MOVEit Transfer which included certain personal data.

What Information Was Involved?

According to our vendor, and our own careful review of the contents of the files impacted, it appears that one or more of the files contained certain of your personal information, specifically your name and one or more of your Leader Bank account numbers. The review of the files received does NOT indicate that any other information (such as social security number, tax identification number, address, telephone number, email, debit card number, date of birth or online banking passwords) were included in this incident.

What We Are Doing.

We wanted to notify you of this incident and to assure you that we take it seriously. Upon learning of this incident, our vendor took immediate steps to launch a comprehensive investigation, and upon receiving notice, Leader Bank itself reviewed all files to identify individuals affected and notified regulatory bodies as required. To help prevent something like this happening again, our vendor has remediated all technical vulnerabilities and patched systems in accordance with the MOVEit software provider's guidelines. Our vendor also mobilized a technical response team to examine the relevant MOVEit Transfer systems and ensure that there were no further vulnerabilities. Leader Bank itself does not use the MOVEit Transfer systems impacted. In addition, Leader Bank has implemented enhanced monitoring of any account number impacted by this incident to help detect any unauthorized activity which could be associated with a third party obtaining this information.

What You Can Do.

We strongly recommend that you closely monitor your Leader Bank accounts for any unusual or unauthorized activity. If you would like to arrange to have your account number(s) changed, please contact at our Client Services team at 781-641-8686 or 855-294-4488, or your local Leader Bank branch directly.

We have arranged for you to receive a complimentary free identity monitoring service through Kroll for two years. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. For more information on identity theft prevention, including instructions on how to activate your identity monitoring, as well as some additional steps you can take for your protection, please review Attachments A and B that follow this letter. Regardless of whether you elect to activate the identity monitoring service, we strongly recommend that you remain vigilant and regularly review and monitor your credit history to guard against any unauthorized transactions or activity.

For More Information.

Please be assured that we are taking steps to address the incident and to help protect the security of your data. If you have any questions about this notice or the incident, please feel free to contact our Client Service team at 781-641-8686 or 855-294-4488, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, Saturdays 9:00 a.m. to 5:00 p.m. Eastern Time, or Sundays, 9:00 am to 2:00 pm Eastern Time, excluding major U.S. holidays.

Sincerely,

Leader Bank, N.A.

ATTACHMENT A

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until November 26, 2023 to activate your identity monitoring services.

Membership Number: [Membership ID]

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com or reach out to our dedicated call center at XXX-XXX-XXXX, from 8:00 am to 5:30 pm CT, excluding some major U.S. holidays, for activation assistance.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ATTACHMENT B

ADDITIONAL STEPS YOU CAN TAKE

To help protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your state's Attorney General, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three consumer reporting agencies below:

Equifax:

Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com

Experian:

Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:

Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
www.transunion.com

Fraud Alert: Consider contacting the three major consumer reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might help protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major consumer reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts 90 days, but can be renewed.

Credit Freeze: A credit freeze prohibits a consumer reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, 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.

Placing a credit freeze is free. To place a credit freeze, contact all three consumer reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

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.); and
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three consumer reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to help protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

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, (860) 808-5318, www.ct.gov/ag.

District of Columbia Residents: The Attorney General can be contacted at the Office of the Attorney General, 441 4th Street NW, Washington, DC 20001; (202) 727-3400; or <https://oag.dc.gov/>.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or <http://www.oag.state.md.us>.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are a victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699- 9001; (919) 716-6400; or <http://www.ncdoj.gov>.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

New York Residents: 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>; and New York State Office of the Attorney General, The Capitol, Albany, NY, 12224-0341, (800) 771-7755, <https://ag.ny.gov>.

Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island Residents: The Attorney General can be contacted at (401) 274-4400 or <http://www.riag.ri.gov/>. You may also file a police report by contacting local or state law enforcement agencies.

Washington Residents: You may contact the Washington State Office of the Attorney General, 1225 Washington St, SE, PO box 40100, Olympia, WA, 98504, <https://www.atg.wa.gov/consumer-issues>, (800) 551-4636 (in Washington only) or (206) 464-6684.

West Virginia Residents: You may contact the West Virginia Attorney General, PO Box 1789, Charleston, WV, 25326-1789, <https://ago.wv.gov/consumerprotection/pages/identity-theft-prevention.aspx>, (800) 368-8808.