

August 10, 2023

Customer  
Address  
City, ST Zip

Re: Incident Notification

On July 12, 2023 Horizon Bank received written notice from a third-party vendor, which provides services to many prominent financial institutions, that its customer data was included in the global incident involving Progress Software MOVEit Transfer, a file transfer software deployed by government agencies and corporations worldwide.

The security of our customers' personal information is our top priority. Immediately upon learning of the incident, we communicated with the third-party vendor to confirm **the incident did not involve Horizon Bank's internal network or IT systems**. We also confirmed the vendor implemented recommended patches released by Progress Software for the MOVEit platform to date. Additionally, we worked with the vendor to identify impacted customers and the extent of information exposed.

As part of our continuing investigation, we discovered an unauthorized third-party did gain access to personally identifiable information of select consumer clients on or about May 30, 2023. While the accessed information is less than that contained on a personal check, out of an abundance of caution, we want to inform you of this incident. The information included name, account number, and an outdated balance. **Customer sensitive information such as social security number, birthdate, on-line banking credentials, or debit card numbers was not contained in the files accessed.**


In addition, we proactively engaged our critical vendors that may have been impacted by the same vulnerability of MOVEit software. While we have not received notification from any other vendor, we will continue to assess and respond to any impacts.

Horizon Bank values our relationship and takes your data privacy very seriously. This is why we have substantial privacy policies and procedures for ourselves and our third-party service providers. As always, and certainly in light of the global nature of the incident surrounding the MOVEit software, we encourage you to be proactive in protecting your personal information:

- Remain vigilant over the next 12-24 months, and carefully review account statements and immediately report any suspicious activity. You may call Horizon Bank at (888) 873-2640 for any assistance or questions.
- Utilize online banking to view transaction activity on a regular basis, including the use of alerts for notification of balance changes, invalid logins, authorized transfers, etc.
- Visit Horizon Bank's Online Security Center to learn more about fraud prevention and security including ways to monitor your credit with the three major credit reporting agencies at [www.horizonbank.com/privacy-and-security](http://www.horizonbank.com/privacy-and-security).
- Visit the Federal Trade Commission's website that explains how to protect your private information at <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>.

We are committed to ensuring the safety and financial success of all our customers and thank you for your trust and relationship with Horizon Bank. Please feel free to reach out if you have any questions.

Sincerely,



Kathie A. DeRuiter,  
Executive Vice President, Senior Operations Officer

## Additional Information

For **Illinois** and **North Carolina** residents, the Federal Trade Commission can be reached at:

Federal Trade Commission  
Bureau of Consumer Protection  
600 Pennsylvania Ave., NW  
Washington, DC 20580  
1-877-438-4338

<https://www.consumer.ftc.gov/features/feature-0014-identity-theft>

For **Illinois, Massachusetts, New Mexico, and North Carolina** residents, the contact information for the three major consumer reporting agencies are as follows:

Equifax	Experian	TransUnion
1.888.298.0045	1.888.397.3742	1.800.916.8800
P.O. Box 740256	P.O. Box 4500	P.O. Box 2000
Atlanta, GA 30348-0256	Allen, TX 75013	Woodlyn, PA 19094
<a href="http://www.equifax.com">www.equifax.com</a>	<a href="http://www.experian.com">www.experian.com</a>	<a href="http://www.transunion.com">www.transunion.com</a>

For **Illinois** residents, you can obtain information about fraud alerts and security freezes from the Federal Trade Commission and the three major consumer reporting agencies.

For **Massachusetts** residents, you have the right to obtain any police report filed in regard to this event. If you are a victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may request a security freeze which would prevent a credit bureau from releasing information in the credit report without your express authorization. It is designed to prevent credit, loans, and services from being approved in your name without your consent. There shall be no charge to place or lift a security freeze on your credit report. To request a security freeze, you may be required to provide the following information: 1. Full name (including middle initial as well as Jr., Sr., II, III, etc.); 2. Social Security number; 3. Date of birth; 4. Addresses for the prior two to 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, etc.); 7. Social Security Card, pay stub, or W2; 8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Should you wish to place a security freeze, please contact the three major consumer reporting agencies listed above.

For **New Mexico** residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.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, you can obtain information about preventing identity theft from the Federal Trade Commission and the New York Attorney General's Office, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and <https://ag.ny.gov/consumerfrauds-bureau/identity-theft>.

For **North Carolina** residents, you can obtain information about preventing identity theft from the Federal Trade Commission and the North Carolina Attorney General's Office. The North Carolina Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 (1-877-5-NO-SCAM); and [www.ncdoj.gov](http://www.ncdoj.gov).