



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Colin D. Scanlon
Office: (267) 930-4259
Fax: (267) 930-4771
Email: cscanlon@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

June 30, 2023

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Union Bank and Trust Company (“UBT”) located at 3643 S 48th St., Lincoln, Nebraska 68501-2535, and are writing to notify your office of an incident that may affect the security of certain personal information relating to eight thousand five hundred seventy-eight (8,578) Iowa residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, UBT does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

On May 31, 2023, UBT was notified by Progress Software of a zero-day vulnerability within their MOVEit Transfer software. UBT immediately took the MOVEit Transfer application offline and initiated an investigation into the nature and scope of the event with the assistance of third-party forensic specialists. The investigation determined the vulnerability identified by Progress Software was exploited and certain customer information being stored within UBT’s MOVEit Transfer application was subject to unauthorized access on May 29, 2023. No other UBT systems were affected by this incident. The information that could have been subject to unauthorized access includes name, address, email address, phone number and Social Security number.

Notice to Iowa Residents

On June 30, 2023, UBT began providing written notice of this incident to eight thousand five hundred seventy-eight (8,578) Iowa residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, UBT moved quickly to investigate, assess the security of its systems, and identify potentially affected individuals. Further, UBT notified federal law enforcement of the event and understands law enforcement has an open investigation. UBT is also working to implement additional safeguards and is providing individuals whose personal information was potentially affected by this incident access to credit monitoring services for twelve (12) months through Kroll at no cost to the individuals.

Additionally, UBT is providing impacted individuals with guidance on how to better protect against identity theft and fraud. UBT is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. UBT is also providing notice of this incident to relevant state and federal regulators and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4259.

Very truly yours,



Colin D. Scanlon of
MULLEN COUGHLIN LLC

CDS/bld
Enclosure

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1 (Notice Of [Data Breach/Security Incident])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Union Bank and Trust Company (“UBT”) writes to notify you of an incident that may affect the privacy of some of your information. This letter provides details of the incident, our response, and steps you may take to better protect against possible misuse of your information, should you feel it appropriate to do so.

What Happened? On May 31, 2023, UBT was notified by Progress Software of a zero-day vulnerability within their MOVEit Transfer software. UBT immediately took the MOVEit Transfer application offline and initiated an investigation into the nature and scope of the event with the assistance of third-party forensic specialists. The investigation determined the vulnerability identified by Progress Software was exploited and certain customer information being stored within UBT’s MOVEit Transfer application was subject to unauthorized access on May 29, 2023. No other UBT systems were affected by this event. UBT was not the only company/organization impacted by this incident. MOVEit software is used throughout many industries. Early reports indicate government agencies and various companies and organizations have experienced similar security events due to the software’s vulnerability.

What Information Was Involved? We determined that the type of information potentially impacted by this incident includes your: <<b2b_text_2 (name and data elements)>>. Please note that the investigation determined no customer accounts or account information was accessed.

What We Are Doing. The confidentiality, privacy, and security of information in our care is among our highest priorities. Upon being notified of the vulnerability, we immediately took steps to secure the information being stored within the application. We also reported the event to federal law enforcement. Moreover, we updated the MOVEit Transfer application with the security patch issued by Progress Software.

As an added precaution, we are offering you access to free identity monitoring services for twelve (12) months through Kroll. The deadline to activate in these services is <<b2b_text_3 (enrollment deadline date)>>. A description of services and instructions on how to activate can be found within the enclosed *Steps You Can Take to Help Protect Your Information*. Please note that you must complete the activation process yourself, as we are not permitted to activate you in these services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements over the next twelve (12) to twenty-four (24) months for suspicious activity and to detect errors.

You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find more information on the credit monitoring and identity restoration services we are making available to you.

For More Information. If you have questions, you can call our dedicated assistance line at [XXX-XXX-XXXX](tel:XXX-XXX-XXXX) between 8:00 a.m. to 5:30 p.m. Central time, Monday through Friday, excluding major U.S. holidays. You can also write to us at P.O. Box 82535, Lincoln, NE 68501-2535. Should you need to report any suspicious activity please feel free to contact your local branch or our customer support team at 1-800-297-2837.

Respectfully,



Angie Muhleisen
President and CEO
Union Bank and Trust Company



Drew Brown
Chief Information Officer
Union Bank and Trust Company

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate in Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. 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.

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

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.



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 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a 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. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

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

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 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, 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 bureaus 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 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfbp_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 New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event. [There are approximately \[#\] Rhode Island residents impacted by this event.](#)