Appendix

On January 19, 2026, Mainstreet Credit Union ("MCU") received an alert from their Managed Security Operations Center that identified suspicious activity related to an employee's email account. MCU immediately instituted their incident response procedure and secured the account. On January 22, 2026, MCU engaged Baker & Hostetler, LLP ("BakerHostetler") to provide legal advice in connection with the event.

On behalf of MCU, BakerHostetler engaged CRA to review forensic evidence from MCU's email environment to determine if any data was accessed during the incident and whether there was unauthorized access to personal information. The investigation confirmed an unauthorized actor accessed one Microsoft 365 account between January 12, 2026, and January 20, 2026. MCU was unable to determine which specific emails and attachments were accessed by the threat actor. MCU reviewed all the emails and attachments that were stored in the account for any personal information. On April 6, 2026, MCU completed its review, which determined that one or more of the emails or attachments included personal information belonging to two Nebraska residents.

On May 4, 2026, MCU began mailing notification letters to the two Nebraska residents via U.S. First-Class mail. MCU is offering complimentary credit monitoring, fraud consultation and identity theft restoration services through Kroll to individuals with Social Security numbers or driver's license numbers involved.

To help prevent similar incidents in the future, MCU will continue to assess its security procedures and training.

mainstreet credit union™

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

SCAN TO ENROLL

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

Dear <<first_name>> <<last_name>>,

Mainstreet Federal Credit Union is writing to make you aware of a data security incident that may have involved some of your information. This letter explains the incident, measures we have taken, and some steps you may consider taking.

We have completed an investigation of suspicious activity associated with one employee email account. Upon identifying the activity, we promptly took steps to secure the account and investigate the activity. We determined that an unauthorized person accessed the account between January 12 and January 20, 2026. While we were unable to determine the specific emails, attachments or files accessed by the threat actor, out of an abundance of caution, we reviewed all the emails and attachments that were stored in the account during the period of compromise for any personal information. On April 6, 2026, we determined that one or more of the emails, attachments, or files contained your <<b2b_text_2 (data elements)>>.

We have secured the services of Kroll to provide identity monitoring at no cost to you for ***12 months***. The identity monitoring services we are making available include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. For more information on identity theft prevention and Kroll's identity monitoring, including instructions on how to activate your complimentary membership, please visit the website below and see the pages that follow this letter.

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

You have until ***<<b2b_text_6 (Date)>>*** *to activate your identity monitoring services.*

Membership Number: **<<Membership Number (S_N)>>**

We remind you that it is always a good idea to be vigilant for incidents of fraud or identity theft by reviewing account statements and free credit reports for any unauthorized activity. Please also review the enclosed *Additional Steps You Can Take*, which contains information about what you can do to safeguard against possible misuse of your information.

We apologize for any concern or inconvenience this incident may cause. We have taken, and will continue to take, steps to enhance the security of our email environment. If you have any questions about this incident, please call (844) 403-4628, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding some major U.S. holidays. Please have your membership number ready.

Sincerely,

Mainstreet Federal Credit Union

KROLL

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. 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.

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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you 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 over the next 12 to 24 months. 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. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-833-799-5355

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. 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.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Mainstreet Credit Union is located at 13001 W. 95th Street Lenexa, KS 66215 and can be reached at 913.599.1010.

Additional Information for Residents of the Following States

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, https://oag.maryland.gov/Pages/oag.aspx