COLLINS & COLLINS, LLC
ATTORNEYS AT LAW

PATRICK J. COLLINS⌖
PATRICE B. COLLINS
ANDREW L. HUNTER
BRIAN G. COLLINS◊
⌖ALSO LICENSED IN ILLINOIS
◊ALSO LICENSED IN NEBRASKA

700 - 17TH STREET
SUITE 1820
DENVER, COLORADO 80202
(303) 296-7700

LAW OFFICE OF
RAYMOND LEAKE, LLC
Of Counsel

LAW OFFICE OF
GERALD J. RAFFERTY, LLC
Of Counsel

ahunter@lawcc.us

March 10, 2023

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

Sent via Email to IDTheft@oag.state.md.us

Re: Security Breach Notification – Arapahoe Credit Union

To Whom it May Concern:

We write this letter to you on behalf of our client, Arapahoe Credit Union ("ACU"). ACU is a credit union located and chartered in Colorado with an address of 3999 E. Arapahoe Road, Littleton, CO 80122. ACU serves a handful of members who reside in Maryland.

On November 30, 2022, ACU discovered that its internal email system may have been breached by an outside entity. ACU immediately launched an investigation in consultation with outside cybersecurity professionals who perform digital forensics to investigate and analyze data breaches to determine the extent of any potential compromise of information on its internal email system.

Based thereon, on January 25, 2023, ACU was informed that an internal email account had been accessed by a hacker who used an application to interface with the compromised account from November 16, 2022 until November 30, 2022. It was discovered that during the breach, the hacker likely had accessed certain member personal identifiable information ("PII"). The credit union had protected its internal email system by using, amongst other things, protected usernames, passwords and Multi-Factor Authentication. The credit union did not allow employees to include member PII in the body or title of an internal email, however attachments were not limited within internal email communications. Most PII revealed in this breach was contained in attached documents.

The PII likely accessed by the hackers from the attachments to ACU internal emails contained member names, Social Security numbers, account numbers and credit card or debit numbers, although none of the account, credit card or debit card numbers contained any security codes, access codes or passwords that would permit access to that account. Not all of the above-listed information was exposed for each member although the compromise did expose these types of PII. The breach potentially affected two ACU members residing in Maryland.

As a result of this compromise, additional security procedures have been implemented or will be implemented soon at ACU. No longer are attachments containing PII allowed, the email will contain a link to a secure network location to access sensitive member documents. [redacted]

After learning the scope of the breach, the credit union proceeded to immediately hire a firm to provide twelve months of credit report monitoring and dark web monitoring with fully managed identity theft for the affected members who opt-in to the service (at no cost to the members). Enclosed is a sample member notice letter which was transmitted to ACU members. ACU has also reported the data breach to both federal and local policing agencies as well as to the National Credit Union Administration.

Please feel free to contact me directly if you have any additional questions or concerns.

Very truly yours,

COLLINS & COLLINS, LLC

Andrew L. Hunter

Cc: Arapahoe Credit Union
Encl.

Arapahoe Credit Union
ArapahoeCU.org Better than Banking...
CENTENNIAL BRANCH
3999 E. Arapahoe Rd.
Centennial, CO 80122
ENGLEWOOD BRANCH
303 E. Hampden Ave.
Englewood, CO 80113
303-740-7063
866-740-7063

February 24, 2023

First Middle Last
Business Name
Address1 Address2
City, State Zip

Dear First Name:

We are writing with important information regarding a recent security incident at Arapahoe Credit Union. The privacy and security of the information we maintain is of the utmost importance to us. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

We discovered unauthorized access to our internal email system may have occurred between November 16, 2022 and November 30, 2022. We immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to determine the extent of any potential compromise of information on our email system. Based thereon, on January 25, 2023, ACU was informed that an internal email account had been compromised which may have resulted in the impermissible exposure of certain member information. While there is no evidence that member information was accessed, it was determined that the content of breach may have included your name, address, Social Security number and/or account number and credit card number(s).

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. However, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity theft, and suggest steps that you should take as well.

As a precautionary measure, we are offering identity theft protection services through NXG, a data security incident and recovery services expert, at no cost to you. The following NXG identity protection services are available to you, free of charge, for one year:

- **Credit Monitoring** that can alert you to new or suspicious activity related to your credit file; and
- **Dark Web Monitoring** to monitor your name, address, Social Security number, and up to 50 other personal credentials, for potential exposure on the dark web; and
- **Fully Managed Identity Theft Recovery**, which will provide professional help in the event you experience any kind of identity theft, either financial or non-financial. A professional Recovery Advocate can help you place fraud alerts, review your credit report, and resolve any incident of identity theft.

IMPORTANT NOTE: Monitoring services require activation in order to go into effect. Please follow the activation instructions on the following page before May 1, 2023 if you wish to take full advantage of these services.

If you have questions about these services or suspect you may be the victim of identity theft, please call the Recovery Care Center at 800-505-5440. Identity Recovery Advocates are available Monday through Friday from 6:00 am to 5:00 pm Mountain Time (MT). Please note the deadline to enroll is April 30, 2023. We continue to urge you to place a password on your ACU accounts, as well as any other financial institution accounts you may own. While there is no evidence any accounts passwords were fraudulently obtained because of this breach, as a precaution, we advise you to change any passwords you may have with us. This letter also provides other precautionary measures you can take to protect your information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

We regret any inconvenience that this security incident has caused. We are committed to maintaining the privacy and security of personal information in our possession and have taken many precautions to safeguard it, including but not limited to improving our endpoint security. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. If you have any further questions regarding this incident, please contact us at 303-740-7063. This response line is staffed with Arapahoe Credit Union employees familiar with this incident and knowledgeable on what you can do to protect against misuse of your information.

OTHER IMPORTANT INFORMATION

1. Enroll in Complimentary 12 Month Credit Monitoring and Dark Web Monitoring.
<u>To activate monitoring and complete authentication, please follow these steps before May 1, 2023</u>.

- Go to https://incidentresponse.merchantsinfo.com
    - click the red button "Sign up takes 3 minutes, WITH INSTANT PROTECTION!"
- Near the bottom of the next screen under "Enroll in a Plan":
    - enter this promotional code: **ARP230277**
    - click the green "Apply" button
- Click the green "Enroll Now" under "ID Theft Protection Individual Coverage"

Follow the instructions on each page to complete your enrollment and online authentication.

In order to authenticate your identity, you may be asked to provide information that is already contained in your credit file. This is to assure that you are the rightful owner of the information. If you have any questions regarding these credit monitoring services or if you encounter a problem while enrolling please call the Recovery Care Center at 800-505-5440.

Remember to always carefully review your statements each month to identify unauthorized transactions. Remain vigilant over the next 12 to 24 months and promptly report incidents of suspected identity theft or unauthorized activity to the appropriate law enforcement agency.

2. Consider Placing a Fraud Alert on Your Credit File. Whether or not you choose to use the complimentary 12-month credit and dark web monitoring services, if you suspect you might be a victim of identity theft, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
(800) 685-1111
www.equifax.com/CreditReportAssistance
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com/fraud
535 Anton Blvd., Ste 100
Costa Mesa, CA 92626

TransUnion
(800) 916-8800
www.transunion.com/fraud
P.O. Box 6790
Fullerton, CA 92834

3. Consider Placing a Security Freeze on Your Credit File. If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax
(800) 685-1111
www.equifax.com/CreditReportAssistance
P.O. Box 105788
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com/freeze
P.O. Box 9701
Allen, TX 75013

TransUnion
(800) 916-8800
www.transunion.com/freeze
P.O. Box 2000
Chester, PA

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtain a Free Credit Report. Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. During these times of COVID-19, Equifax, Experian, and TransUnion are now offering free weekly online reports. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources. You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). You may also visit identitytheft.gov for additional resources and advice on next steps.

If this notice letter states that your Arapahoe Credit Union account information was impacted, we recommend that you contact us at 303-740-7063 to inquire about steps to take to protect your account.

Sincerely,

Christine Eckhardt
Chief Operations Officer
www.ArapahoeCU.org

Arapahoe Credit Union
ArapahoeCU.org Better than Banking...
CENTENNIAL BRANCH
3999 E. Arapahoe Rd.
Centennial, CO 80122
ENGLEWOOD BRANCH
303 E. Hampden Ave.
Englewood, CO 80113
303-740-7063
866-740-7063

February 24, 2023

First Middle Last
Business Name
Address1 Address2
City, State Zip

Dear First Name:

We are writing with important information regarding a recent security incident at Arapahoe Credit Union. The privacy and security of the information we maintain is of the utmost importance to us. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

We discovered unauthorized access to our internal email system may have occurred between November 16, 2022 and November 30, 2022. We immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to determine the extent of any potential compromise of information on our email system. Based thereon, on January 25, 2023, ACU was informed that an internal email account had been compromised which may have resulted in the impermissible exposure of certain member information. While there is no evidence that member information was accessed, it was determined that the content of breach may have included your name, address, social security number and/or account number.

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. However, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity theft, and suggest steps that you should take as well.

As a precautionary measure, we are offering identity theft protection services through NXG, a data security incident and recovery services expert, at no cost to you. The following NXG identity protection services are available to you, free of charge, for one year:

- **Credit Monitoring** that can alert you to new or suspicious activity related to your credit file; and
- **Dark Web Monitoring** to monitor your name, address, Social Security number, and up to 50 other personal credentials, for potential exposure on the dark web; and
- **Fully Managed Identity Theft Recovery**, which will provide professional help in the event you experience any kind of identity theft, either financial or non-financial. A professional Recovery Advocate can help you place fraud alerts, review your credit report, and resolve any incident of identity theft.

IMPORTANT NOTE: Monitoring services require activation in order to go into effect. Please follow the activation instructions on the following page before May 1, 2023 if you wish to take full advantage of these services.

If you have questions about these services or suspect you may be the victim of identity theft, please call the Recovery Care Center at 800-505-5440. Identity Recovery Advocates are available Monday through Friday from 6:00 am to 5:00 pm Mountain Time (MT). Please note the deadline to enroll is April 30, 2023. We continue to urge you to place a password on your ACU accounts, as well as any other financial institution accounts you may own. While there is no evidence any accounts passwords were fraudulently obtained because of this breach, as a precaution, we advise you to change any passwords you may have with us. This letter also provides other precautionary measures you can take to protect your information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

We regret any inconvenience that this security incident has caused. We are committed to maintaining the privacy and security of personal information in our possession and have taken many precautions to safeguard it, including but not limited to improving our endpoint security. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information. If you have any further questions regarding this incident, please contact us at 303-740-7063. This response line is staffed with Arapahoe Credit Union employees familiar with this incident and knowledgeable on what you can do to protect against misuse of your information.

OTHER IMPORTANT INFORMATION

1. Enroll in Complimentary 12 Month Credit Monitoring and Dark Web Monitoring.
To activate monitoring and complete authentication, please follow these steps before May 1, 2023.

- Go to https://incidentresponse.merchantsinfo.com
    - click the red button "Sign up takes 3 minutes, WITH INSTANT PROTECTION!"
- Near the bottom of the next screen under "Enroll in a Plan":
    - enter this promotional code **ARP230277**
    - click the green "Apply" button
- Click the green button "Enroll Now" under "ID Theft Protection Individual Coverage"

Follow the instructions on each page to complete your enrollment and online authentication.

In order to authenticate your identity, you may be asked to provide information that is already contained in your credit file. This is to assure that you are the rightful owner of the information. If you have any questions regarding these credit monitoring services or if you encounter a problem while enrolling please call the Recovery Care Center at 800-505-5440.

Remember to always carefully review your statements each month to identify unauthorized transactions. Remain vigilant over the next 12 to 24 months and promptly report incidents of suspected identity theft or unauthorized activity to the appropriate law enforcement agency.

2. Consider Placing a Fraud Alert on Your Credit File. Whether or not you choose to use the complimentary 12-month credit and dark web monitoring services, if you suspect you might be a victim of identity theft, we recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
(800) 685-1111
www.equifax.comCreditReportAssistance
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com/fraud
535 Anton Blvd., Ste 100
Costa Mesa, CA 92626

TransUnion
(800) 916-8800
www.transunion.com/fraud
P.O. Box 6790
Fullerton, CA 92834

3. Consider Placing a Security Freeze on Your Credit File. If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax
(800) 685-1111
www.equifax.com/CreditReportAssistance
P.O. Box 105788
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com/freeze
P.O. Box 9701
Allen, TX 75013

TransUnion
(800) 916-8800
www.transunion.com/freeze
P.O. Box 2000
Chester, PA

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtain a Free Credit Report. Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. During these times of COVID-19, Equifax, Experian, and TransUnion are now offering free weekly online reports. Call 1-877-322-8228 or request your free credit reports online at www.annualcreditreport.com. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources. You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). You may also visit identitytheft.gov for additional resources and advice on next steps.

If this notice letter states that your Arapahoe Credit Union account information was impacted, we recommend that you contact us at 303-740-7063 to inquire about steps to take to protect your account.

Sincerely,

Christine Eckhardt
Chief Operations Officer
www.ArapahoeCU.org