

EXHIBIT 1

By providing this notice, Vizo Financial Corporate Credit Union (“Vizo Financial”) does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

As discussed in our letter dated July 30, 2020, previously provided to you (attached here as *Exhibit B*), Vizo Financial provides core accounting services to approximately 800 credit unions. In connection with providing these services, Vizo Financial receives information from its affiliated credit unions including personal information relating to the credit union’s members. On May 5, 2020, Vizo Financial became aware of suspicious activity related to an employee’s email account. In response, they immediately took additional steps to enhance the security of our email system and began working with outside computer forensics specialists to determine the nature and scope of the incident. The investigation determined that two Vizo Financial employee email accounts were accessed by an unauthorized actor on February 26, 2020, and April 2, 2020, respectively. An additional comprehensive review was undertaken to determine those email messages and file attachments in the impacted email accounts that were at risk for unauthorized access and to identify any personal information present. Once this exhaustive review was complete, Vizo Financial then worked diligently to confirm to which of its member credit unions the potentially impacted personal information related.

On or about June 15, 2020, Vizo Financial confirmed the population of potentially impacted credit union members and their affiliated credit unions. Although the type of personal information potentially impacted for impacted members may vary by individual, the following types of personal information were potentially impacted as a result of this incident: name and bank account information.

Notice to Maine Resident

On June 24, 2020, Vizo Financial provided written notice of the incident to the impacted credit unions and offered to provide written notification to impacted credit union members on behalf of the credit unions. Written notice to the impacted credit unions was provided in substantially the same form as the letter attached hereto as *Exhibit A*. Written notification to the impacted credit union members was provided in substantially the same form as the letter attached as *Exhibit A-1*.

Following responses from its impacted customer credit unions, Vizo Financial coordinated mailing to impacted credit union members on behalf of those credit unions who elected to have Vizo Financial do so. Of the total impacted individuals notified, one (1) individual affiliated with one (1) credit union is a resident of Maine. Notice to this individual was provided on July 23, 2020. At this time, the investigation of and response to the event is complete. Accordingly, in order to supplement the prior notification provided on July 30, 2020, Vizo Financial provides the instant notification to the Office of the Maine Attorney General to complete the requisite notification obligations resulting from this event regarding the impacted Maine resident.

Other Steps Taken and To Be Taken

Upon discovering the suspicious activity in its email system, Vizo Financial immediately took steps to secure the affected accounts and worked with third-party forensic investigators to review and secure its entire network. Additionally, while Vizo Financial has safeguards in place to protect the data in its care, as part of its ongoing commitment to the security of information in its care, Vizo Financial is reviewing and enhancing policies and procedures to reduce the likelihood of a similar event in the future, including implementing multifactor authentication for all administrative level accounts across the Vizo Financial environment. Vizo Financial also reported this incident to appropriate regulatory authorities, including its federal regulatory authority, the National Credit Union Administration, and its state regulatory authority, the North Carolina Credit Union Division.

As an added precaution, Vizo Financial offered all domestic credit union members access to twenty-four (24) months of complimentary identity monitoring services for through Experian. Further, Vizo Financial provided impacted credit union members with guidance on how to better protect against identity theft and fraud, including 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 identity theft and fraud 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.

EXHIBIT A



[First Name] [Middle Name] [Last Name] [Suffix]
[Credit Union Name]
[Address Line 1]
[Address Line 2]
[City], [State] [Zip]

[Date]

Re: Notice of Data Security Incident

Dear [Credit Union Contact's Name],

Vizo Financial Corporate Credit Union (“Vizo Financial”) writes to inform your credit union of a recent data security incident that may impact the security of personal information of approximately [] (#) of your current or former members. Vizo Financial holds the privacy and protection of personal information in our care among our highest priorities, and we are dedicated to providing our member credit unions with the highest standards in service. Although we have no indication of misuse of personal information relating to this incident, we are providing you with information about the incident and steps we are taking in response, which includes an offer for Vizo Financial to handle certain next steps that may be required of your organization, such as providing notice of the incident to your impacted members.

What Happened? On May 5, 2020, Vizo Financial became aware of suspicious activity related to an employee’s email account. In response, we immediately took additional steps to enhance the security of our email system and began working with outside computer forensics specialists to determine the nature and scope of the incident. The investigation determined that two Vizo Financial employee email accounts were accessed by an unauthorized actor on February 26, 2020, and April 2, 2020, respectively. An additional comprehensive review was undertaken to determine those email messages and file attachments in the impacted email accounts that were at risk for unauthorized access and to identify any personal information present. Once this exhaustive review was complete, we then worked diligently to confirm which of our member credit unions the potentially impacted personal information related.

What Information Was Involved? On or about June 15, 2020, we confirmed the population of potentially impacted credit union members and their affiliated credit unions. Our investigation determined that personal information relating to [number of impacted members] of your members was present in the email accounts and may have been subject to unauthorized access. Although the type of personal information potentially impacted for your members may vary by individual, the following types of personal information were potentially impacted for your members: name and bank account information. Together with this email, we are providing you with a complete list of the names of your impacted members and their address information to the extent it was present.

What is Vizo Financial Doing? We take this incident and the security of personal information in our care very seriously. Upon discovering the suspicious activity in our email system, we immediately took additional steps to secure the affected accounts and worked with third-party forensic investigators to review

7900 Triad Center Drive
Suite 410
Greensboro, NC 27409
(800) 585-4317

1201 Fulling Mill Road
Middletown, PA 17057
(800) 622-7494
www.vfccu.org

and secure our entire network. Additionally, while we have safeguards in place to protect the data in our care, as part of our ongoing commitment to the security of information in our care, we are reviewing and enhancing policies and procedures to reduce the likelihood of a similar event in the future, including implementing multifactor authentication for all administrative level accounts across the Vizo Financial environment. We also reported this incident to appropriate regulatory authorities, including the National Credit Union Administration and the North Carolina Credit Union Division.

Vizo Financial's Offer to Satisfy Additional Required Steps: In response to this incident, and subject to your organization's authorization, Vizo Financial is offering to provide notice to your potentially affected credit union members. This notice will include information on the incident and steps these members can take to protect themselves from identity theft, as outlined in the attached sample notice letter. Moreover, as an added precaution, Vizo Financial is offering all eligible impacted members access to twenty-four (24) months of complimentary identity monitoring services for through Experian.

Please let us know by July 31, 2020 whether you would like Vizo Financial to notify potentially affected members on your behalf. Vizo Financial will pay for costs associated with providing notice to your impacted members, including fees associated with the offered credit monitoring services. Please note, as reflected on the attached list of your impacted members, Vizo Financial may not have address information for all potentially affected individuals. If your organization is able to supplement the available address information for your potentially affected members, at your direction, Vizo Financial will mail notification letters to those individuals as well. We ask that you kindly review and confirm and/or revise the address information, and return it to your corporate account manager at your earliest convenience.

Please note, Vizo Financial will not notify potentially impacted members on your behalf, unless and until you direct Vizo Financial to do so. Please contact your corporate account manager to provide authorization. We are happy to coordinate with you on the manner and content of these notifications. Further, we note that this event may impose upon your credit union an obligation to notify the National Credit Union Administration, applicable state regulatory authorities, or both. Should it be determined that the NCUA or a state regulator is required to be notified, we would be happy to assist you with satisfying the notification obligations.

We recognize you may have additional questions not addressed by this letter. If you have questions regarding this notification or the proposed notification materials, please call our dedicated call center at 877-890-9162 as soon as possible to discuss. The dedicated call center is open Monday through Friday, from 9:00 a.m. to 11:00 p.m. Eastern Time, and Saturday and Sunday from 11 am to 8 pm Eastern Time, excluding U.S. holidays. Please provide **Engagement # DB20757** when you call. The dedicated call center will be able to answer your questions regarding the event, the steps Vizo Financial took in response, and the assistance Vizo Financial is offering to **_____ Credit Union.**

We sincerely regret any inconvenience this incident may cause you. We remain committed to safeguarding the information in our care and we will continue to take steps to ensure the security of our systems.

Sincerely,



Lori A. Gall
Chief Risk Officer
Vizo Financial Corporate Credit Union

Encl: SAMPLE INDIVIDUAL MEMBER NOTICE LETTER

EXHIBIT A-1



SAMPLE INDIVIDUAL MEMBER NOTICE LETTER

[First Name] [Middle Name] [Last Name] [Suffix]
[Address Line 1]
[Address Line 2]
[City], [State] [Zip]

[Date]

Re: Notice of Data Breach

Dear [First Name] [Middle Name] [Last Name] [Suffix],

Vizo Financial Corporate Credit Union (“Vizo Financial”) is writing on behalf of _____ Credit Union (credit union name) to inform you of a recent event that may impact the security of some of your information. Vizo Financial provides core accounting services to approximately 800 credit unions across the country, including _____ Credit Union (credit union name). In connection with providing these services, Vizo Financial receives information from its affiliated credit unions including personal information relating to the credit union’s members. Although we are unaware of any actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On May 5, 2020, Vizo Financial became aware of suspicious activity related to an employee’s email account. In response, we immediately took additional steps to enhance the security of our email system and began working with outside computer forensics specialists to determine the nature and scope of the incident. The investigation determined that two Vizo Financial employee email accounts were accessed by an unauthorized actor on February 26, 2020, and April 2, 2020, respectively. An additional comprehensive review was undertaken to determine those email messages and file attachments in the impacted email account that were at risk for unauthorized access and to identify any personal information present. Once this exhaustive review was complete, we then worked diligently to confirm to which of our member credit unions the potentially impacted personal information related.

What Information Was Involved? Our investigation determined that the following types of information relating to you were present in the email accounts and therefore accessible to the unknown actor during this incident: name and bank account information. To date, we are unaware of any actual or attempted misuse of your personal information as a result of this incident.

What Vizo Financial is Doing. We take this incident and the security of the personal information entrusted to us, including your personal information, seriously. Upon learning of this incident, we immediately took additional steps to secure the affected email accounts and worked with third-party forensic investigators to review and secure our entire network. Additionally, while we have safeguards in place to protect the data in our care, as part of our ongoing commitment to the security of information in our care, we are reviewing and enhancing policies and procedures to reduce the likelihood of a similar event in the future, including implementing multifactor authentication for all administrative level accounts across the Vizo Financial

7900 Triad Center Drive
Suite 410
Greensboro, NC 27409
(800) 585-4317

1201 Fulling Mill Road
Middletown, PA 17057
(800) 622-7494
www.vfccu.org


environment. Moreover, as an added precaution, while Vizo Financial is unaware of any actual misuse of the information impacted in this incident, Vizo Financial is offering all eligible impacted members access to twenty-four (24) months of complimentary identity monitoring services for through Experian.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanations of benefits, and credit reports for suspicious activity. You may also review the information in the attached “*Steps You Can Take to Help Protect Your Information.*” There you will also find more information on the complimentary identity monitoring services Vizo Financial is making available to eligible members. If eligible, we encourage you to enroll in these credit monitoring and identity theft restoration services that we are offering, as we are not able to act on your behalf to do so.

For More Information. We recognize you may have additional questions not addressed by this letter. If you have additional questions, please call our dedicated assistance line at xxx-xxx-xxxx. The dedicated call center is open Monday through Friday, from 9:00 a.m. to 11:00 p.m. Eastern Time, and Saturday and Sunday from 11 am to 8 pm Eastern Time, excluding U.S. holidays. Please provide **Engagement # [engagement #]** when you call.

We sincerely regret any inconvenience this incident may cause you. We remain committed to safeguarding the information in our care and we will continue to take steps to ensure the security of our systems.

Sincerely,

A handwritten signature in cursive script, appearing to read "Lori A. Gall".

Lori A. Gall
Chief Risk Officer
Vizo Financial Corporate Credit Union

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering a complimentary twenty-four-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: September 30, 2020** – please note your code will not work after this date
- **Visit** the Experian IdentityWorks website to enroll: [URL]
- Provide your **activation code: [code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **xxx-xxx-xxxx by September 30, 2020**. Be prepared to provide engagement number [engagement #] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [xxx-xxx-xxxx]. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

In addition to enrolling to receiving the complimentary services detailed above, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your credit reports for suspicious activity and to detect errors. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

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, provide 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.);
7. 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.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-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 agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19106
1-800-680-7289

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.transunion.com/fraud-victim-resource/place-fraud-alert www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also 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. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; (888) 743-0023; and www.oag.state.md.us.

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 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_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 North Carolina residents, North Carolina residents may wish to review information provided by the North Carolina Attorney General, Consumer Protection Division at www.ncdoj.gov, by calling 877-566-7226, or writing to 9001 Mail Services Center, Raleigh, NC 27699.

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is/are ___ approximately Rhode Island resident/residents impacted by this incident.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

EXHIBIT B



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Alexander T. Walker
Office: (267) 930-4801
Fax: (267) 930-4771
Email: awalker@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

July 30, 2020

VIA E-MAIL

Office of the Maine Attorney General
Security Breach Notification
Consumer Protection Division
111 Sewall Street, 6th Floor
Augusta, ME 04330
E-mail: breach.security@maine.gov

Re: Notice of Data Privacy Event

Dear Sir or Madam:

We represent Vizo Financial Corporate Credit Union (“Vizo Financial”), headquartered at 7900 Triad Center Drive, Suite 410, Greensboro, NC 27409, and are writing to preliminarily notify your office of an incident that may affect the security of personal information relating to residents of your state. This notice may be supplemented if significant facts are learned subsequent to its submission. By providing this notice, Vizo Financial does not waive any rights or defenses regarding the applicability of Maine law or personal jurisdiction.

Notice of the Data Breach

Vizo Financial provides core accounting services to approximately eight hundred (800) credit unions. In connection with providing these services, Vizo Financial receives information from its affiliated credit unions including personal information relating to the credit union members. On May 5, 2020, Vizo Financial became aware of suspicious activity related to an employee’s email account. In response, Vizo Financial immediately took additional steps to enhance the security of our email system and began working with outside computer forensics specialists to determine the nature and scope of the incident. The investigation determined that two Vizo Financial employee email accounts were accessed by an unauthorized actor on February 26, 2020, and April 2, 2020, respectively. An additional

comprehensive review was undertaken to determine those email messages and file attachments in the impacted email account that were at risk for unauthorized access and to identify any personal information present. Once this exhaustive review was complete, Vizo Financial then worked diligently to confirm to which of its member credit unions the potentially impacted personal information related.

On or about June 15, 2020, Vizo Financial confirmed the population of potentially impacted credit union members and their affiliated credit unions. In total, information relating to approximately five hundred and fifteen (515) individual members affiliated with one hundred and thirty-three (133) of Vizo Financial's member credit unions were impacted as a result of this event. Although the type of personal information potentially impacted for impacted members may vary by individual, the following types of personal information were potentially impacted as a result of this incident: name and bank account information.

Notice of Data Privacy Event

On June 24, 2020, Vizo Financial provided written notice of the incident to the impacted credit unions and offered to provide written notification to impacted credit union members on behalf of the credit unions. Written notice to the impacted credit unions was provided in substantially the same form as the letter attached hereto as *Exhibit A*. The proposed written notification to impacted credit union members is attached as *Exhibit A-1*. Vizo Financial is now in the process of coordinating mailing to impacted credit union members on behalf of those credit unions who elected to have Vizo Financial do so. While the notification process is ongoing, to date, notifications to two hundred twenty three (223) individuals affiliated with sixty-one (61) credit unions have been provided. Of this total, one (1) individual affiliated with one (1) credit union is a resident of Maine. A complete list of the one hundred and thirty-three (133) impacted credit unions is attached as *Exhibit B*.

Other Steps Taken and to Be Taken

Upon discovering the suspicious activity in its email system, Vizo Financial immediately took steps to secure the affected accounts and worked with third-party forensic investigators to review and secure its entire network. Additionally, while Vizo Financial has safeguards in place to protect the data in its care, as part of its ongoing commitment to the security of information in its care, Vizo Financial is reviewing and enhancing policies and procedures to reduce the likelihood of a similar event in the future, including implementing multifactor authentication for all administrative level accounts across the Vizo Financial environment. Vizo Financial also reported this incident to appropriate regulatory authorities, including its federal regulatory authority, the National Credit Union Administration, and its state regulatory authority, the North Carolina Credit Union Division.

As an added precaution, Vizo Financial is offering all domestic credit union members access to twenty-four (24) months of complimentary identity monitoring services for through Experian. Further, Vizo Financial is providing impacted credit union members with guidance on how to better protect against identity theft and fraud, including 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 identity theft and fraud 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data breach, please contact us at 267-930-4801.

Very truly yours,

A handwritten signature in black ink, appearing to read "Alexander T. Walker".

Alexander T. Walker of
MULLEN COUGHLIN LLC

ATW/smm
Enclosures

EXHIBIT A

TO THE JULY 30, 2020 NOTIFICATION



[First Name] [Middle Name] [Last Name] [Suffix]
[Credit Union Name]
[Address Line 1]
[Address Line 2]
[City], [State] [Zip]

[Date]

Re: Notice of Data Security Incident

Dear [Credit Union Contact's Name],

Vizo Financial Corporate Credit Union (“Vizo Financial”) writes to inform your credit union of a recent data security incident that may impact the security of personal information of approximately [] (#) of your current or former members. Vizo Financial holds the privacy and protection of personal information in our care among our highest priorities, and we are dedicated to providing our member credit unions with the highest standards in service. Although we have no indication of misuse of personal information relating to this incident, we are providing you with information about the incident and steps we are taking in response, which includes an offer for Vizo Financial to handle certain next steps that may be required of your organization, such as providing notice of the incident to your impacted members.

What Happened? On May 5, 2020, Vizo Financial became aware of suspicious activity related to an employee’s email account. In response, we immediately took additional steps to enhance the security of our email system and began working with outside computer forensics specialists to determine the nature and scope of the incident. The investigation determined that two Vizo Financial employee email accounts were accessed by an unauthorized actor on February 26, 2020, and April 2, 2020, respectively. An additional comprehensive review was undertaken to determine those email messages and file attachments in the impacted email accounts that were at risk for unauthorized access and to identify any personal information present. Once this exhaustive review was complete, we then worked diligently to confirm which of our member credit unions the potentially impacted personal information related.

What Information Was Involved? On or about June 15, 2020, we confirmed the population of potentially impacted credit union members and their affiliated credit unions. Our investigation determined that personal information relating to [number of impacted members] of your members was present in the email accounts and may have been subject to unauthorized access. Although the type of personal information potentially impacted for your members may vary by individual, the following types of personal information were potentially impacted for your members: name and bank account information. Together with this email, we are providing you with a complete list of the names of your impacted members and their address information to the extent it was present.

What is Vizo Financial Doing? We take this incident and the security of personal information in our care very seriously. Upon discovering the suspicious activity in our email system, we immediately took additional steps to secure the affected accounts and worked with third-party forensic investigators to review

7900 Triad Center Drive
Suite 410
Greensboro, NC 27409
(800) 585-4317

1201 Fulling Mill Road
Middletown, PA 17057
(800) 622-7494
www.vfccu.org

and secure our entire network. Additionally, while we have safeguards in place to protect the data in our care, as part of our ongoing commitment to the security of information in our care, we are reviewing and enhancing policies and procedures to reduce the likelihood of a similar event in the future, including implementing multifactor authentication for all administrative level accounts across the Vizo Financial environment. We also reported this incident to appropriate regulatory authorities, including the National Credit Union Administration and the North Carolina Credit Union Division.

Vizo Financial's Offer to Satisfy Additional Required Steps: In response to this incident, and subject to your organization's authorization, Vizo Financial is offering to provide notice to your potentially affected credit union members. This notice will include information on the incident and steps these members can take to protect themselves from identity theft, as outlined in the attached sample notice letter. Moreover, as an added precaution, Vizo Financial is offering all eligible impacted members access to twenty-four (24) months of complimentary identity monitoring services for through Experian.

Please let us know by July 31, 2020 whether you would like Vizo Financial to notify potentially affected members on your behalf. Vizo Financial will pay for costs associated with providing notice to your impacted members, including fees associated with the offered credit monitoring services. Please note, as reflected on the attached list of your impacted members, Vizo Financial may not have address information for all potentially affected individuals. If your organization is able to supplement the available address information for your potentially affected members, at your direction, Vizo Financial will mail notification letters to those individuals as well. We ask that you kindly review and confirm and/or revise the address information, and return it to your corporate account manager at your earliest convenience.

Please note, Vizo Financial will not notify potentially impacted members on your behalf, unless and until you direct Vizo Financial to do so. Please contact your corporate account manager to provide authorization. We are happy to coordinate with you on the manner and content of these notifications. Further, we note that this event may impose upon your credit union an obligation to notify the National Credit Union Administration, applicable state regulatory authorities, or both. Should it be determined that the NCUA or a state regulator is required to be notified, we would be happy to assist you with satisfying the notification obligations.

We recognize you may have additional questions not addressed by this letter. If you have questions regarding this notification or the proposed notification materials, please call our dedicated call center at 877-890-9162 as soon as possible to discuss. The dedicated call center is open Monday through Friday, from 9:00 a.m. to 11:00 p.m. Eastern Time, and Saturday and Sunday from 11 am to 8 pm Eastern Time, excluding U.S. holidays. Please provide **Engagement # DB20757** when you call. The dedicated call center will be able to answer your questions regarding the event, the steps Vizo Financial took in response, and the assistance Vizo Financial is offering to **_____ Credit Union.**

We sincerely regret any inconvenience this incident may cause you. We remain committed to safeguarding the information in our care and we will continue to take steps to ensure the security of our systems.

Sincerely,



Lori A. Gall
Chief Risk Officer
Vizo Financial Corporate Credit Union

Encl: SAMPLE INDIVIDUAL MEMBER NOTICE LETTER

EXHIBIT A-1

TO THE JULY 30, 2020 NOTIFICATION



SAMPLE INDIVIDUAL MEMBER NOTICE LETTER

[First Name] [Middle Name] [Last Name] [Suffix]
[Address Line 1]
[Address Line 2]
[City], [State] [Zip]

[Date]

Re: Notice of Data Breach

Dear [First Name] [Middle Name] [Last Name] [Suffix],

Vizo Financial Corporate Credit Union (“Vizo Financial”) is writing on behalf of _____ Credit Union (credit union name) to inform you of a recent event that may impact the security of some of your information. Vizo Financial provides core accounting services to approximately 800 credit unions across the country, including _____ Credit Union (credit union name). In connection with providing these services, Vizo Financial receives information from its affiliated credit unions including personal information relating to the credit union’s members. Although we are unaware of any actual misuse of your information, we are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On May 5, 2020, Vizo Financial became aware of suspicious activity related to an employee’s email account. In response, we immediately took additional steps to enhance the security of our email system and began working with outside computer forensics specialists to determine the nature and scope of the incident. The investigation determined that two Vizo Financial employee email accounts were accessed by an unauthorized actor on February 26, 2020, and April 2, 2020, respectively. An additional comprehensive review was undertaken to determine those email messages and file attachments in the impacted email account that were at risk for unauthorized access and to identify any personal information present. Once this exhaustive review was complete, we then worked diligently to confirm to which of our member credit unions the potentially impacted personal information related.

What Information Was Involved? Our investigation determined that the following types of information relating to you were present in the email accounts and therefore accessible to the unknown actor during this incident: name and bank account information. To date, we are unaware of any actual or attempted misuse of your personal information as a result of this incident.

What Vizo Financial is Doing. We take this incident and the security of the personal information entrusted to us, including your personal information, seriously. Upon learning of this incident, we immediately took additional steps to secure the affected email accounts and worked with third-party forensic investigators to review and secure our entire network. Additionally, while we have safeguards in place to protect the data in our care, as part of our ongoing commitment to the security of information in our care, we are reviewing and enhancing policies and procedures to reduce the likelihood of a similar event in the future, including implementing multifactor authentication for all administrative level accounts across the Vizo Financial

7900 Triad Center Drive
Suite 410
Greensboro, NC 27409
(800) 585-4317

1201 Fulling Mill Road
Middletown, PA 17057
(800) 622-7494
www.vfccu.org


environment. Moreover, as an added precaution, while Vizo Financial is unaware of any actual misuse of the information impacted in this incident, Vizo Financial is offering all eligible impacted members access to twenty-four (24) months of complimentary identity monitoring services for through Experian.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanations of benefits, and credit reports for suspicious activity. You may also review the information in the attached “*Steps You Can Take to Help Protect Your Information.*” There you will also find more information on the complimentary identity monitoring services Vizo Financial is making available to eligible members. If eligible, we encourage you to enroll in these credit monitoring and identity theft restoration services that we are offering, as we are not able to act on your behalf to do so.

For More Information. We recognize you may have additional questions not addressed by this letter. If you have additional questions, please call our dedicated assistance line at xxx-xxx-xxxx. The dedicated call center is open Monday through Friday, from 9:00 a.m. to 11:00 p.m. Eastern Time, and Saturday and Sunday from 11 am to 8 pm Eastern Time, excluding U.S. holidays. Please provide **Engagement # [engagement #]** when you call.

We sincerely regret any inconvenience this incident may cause you. We remain committed to safeguarding the information in our care and we will continue to take steps to ensure the security of our systems.

Sincerely,

A handwritten signature in cursive script, appearing to read "Lori A. Gall".

Lori A. Gall
Chief Risk Officer
Vizo Financial Corporate Credit Union

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering a complimentary twenty-four-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: September 30, 2020** – please note your code will not work after this date
- **Visit** the Experian IdentityWorks website to enroll: [URL]
- Provide your **activation code: [code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **xxx-xxx-xxxx by September 30, 2020**. Be prepared to provide engagement number [engagement #] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [xxx-xxx-xxxx]. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

In addition to enrolling to receiving the complimentary services detailed above, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your credit reports for suspicious activity and to detect errors. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

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, provide 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.);
7. 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.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-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 agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19106
1-800-680-7289

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.transunion.com/fraud-victim-resource/place-fraud-alert www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also 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. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; (888) 743-0023; and www.oag.state.md.us.

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 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_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 North Carolina residents, North Carolina residents may wish to review information provided by the North Carolina Attorney General, Consumer Protection Division at www.ncdoj.gov, by calling 877-566-7226, or writing to 9001 Mail Services Center, Raleigh, NC 27699.

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is/are ___ approximately Rhode Island resident/residents impacted by this incident.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

EXHIBIT B

TO THE JULY 30, 2020 NOTIFICATION

1st Ed Credit Union
A & S FCU
Access Credit Union
ALCOSE Credit Union
American Partners FCU
American Spirit FCU
AMERICO Federal Credit Union
Anderson FCU
Ardent Federal Credit Union
Argent Federal Credit Union
Armco Credit Union
Arrowpointe Federal Credit Union
Bay Atlantic FCU
Belco Community Credit Union
BENCHMARK FCU
BHCU
Blue Flame Credit Union
Bronco FCU
CACL FCU
Caro Federal Credit Union
Carolina FCU
Carolinas Telco FCU
Central Keystone FCU
Central Virginia FCU
Century Heritage FCU
Charlotte Fire Dept Credit Union
Chrome Federal Credit Union
Community Financial Services FCU
Community Powered Federal Credit
Union
Credit Union Mortgage Association
CS Credit Union
DC Federal Credit Union
Dept of Labor FCU
Destinations Credit Union
Dominion Energy CU
Duke University FCU
Eagle One FCU
EP Federal Credit Union
First Capital FCU
First Carolina People's Credit Union
First Choice FCU

Fort Dix FCU
Franklin-Johnstown FCU
Freedom Credit Union
Freedom United FCU
Frick Tri-County FCU
Garden State F.C.U.
Geico Federal Credit Union
Georgetown Federal Credit Union
GHS Federal Credit Union
GNC Community FCU
Greensboro Municipal Credit Union
Greenville Heritage FCU
Hampton Roads Educators CU, Inc
Hazleton School Emp CU
Healthcare Systems FCU
Heritage Valley FCU
Hidden River Credit Union
HopeSouth Federal Credit Union
HUD Federal Credit Union
IBEW #26 FCU
Inspire Federal Credit Union
Jessop Community FCU
Lakehurst Naval FCU
Lancaster Red Rose CU
Lanco FCU
Latitude32 Credit Union
Lehigh Valley Educators CU
Lexington Avenue FCU
Liberty Savings FCU
Lion's Share Federal Credit Union
Long Reach FCU
L'Oreal USA FCU
Loudoun CU
Marine FCU
Members Choice Financial Credit
Union
Members First of Maryland FCU
Merck Sharp & Dohme FCU
Mountain Credit Union
Mountain Laurel FCU
MTC Federal Credit Union
NE PA Community FCU
NET FCU

Nova Credit Union
Nucor Emp Credit Union
OAS Staff FCU
Oteen VA Federal Credit Union
P & G Mehoopany Emp FCU
PALCO FCU
Palmetto First Credit Union
Palmetto Health Credit Union
Patent & Trademark Office FCU
Penn East FCU
Penn State FCU
Pennsylvania Central FCU
Peoples Advantage FCU
Pheple Federal Credit Union
Philadelphia Letter Carriers FCU
Priority First FCU
Research 1166 FCU
Riegelwood FCU
Riverfront FCU
Riverset Credit Union
Roanoke Valley FCU
Salem VA Med. Center FCU
Service 1st FCU
SkyPoint Federal Credit Union
SPE FCU
Spirit Financial Credit Union
Sun East FCU
Telco Credit Union
Tendto Credit Union
Thiokol Elkton FCU
Tri-Valley Service FCU
Turbine FCU
UFCW Community Federal Credit
Union
University of Pennsylvania Students
FCU
Upstate Credit Union
URW Community FCU
USSCO Johnstown FCU
USX FCU
Utilities Employees CU
ValleyStar CU
Vantage Point FCU

Virginia Credit Union
Visionary Federal Credit Union
VITAL Federal Credit Union
Wawa Employees CU
West-Aircomm FCU
Weyco Community Credit Union
White Rose Credit Union
Yogaville FCU