



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Gregory Lederman
Office: (267) 930-4637
Fax: (267) 930-4771
Email: glederman@mullen.law

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

May 8, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Provident Credit Union (“PCU”), located at 303 Twin Dolphin Drive, Redwood City, CA 94065, and are writing to notify your Office of an incident that may affect the security of certain information relating to two (2) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, PCU does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about September 23, 2022, PCU learned that an employee inadvertently sent an electronic document to a PCU member via a secure messaging portal that included check images that were deposited to other PCU member accounts. Upon learning of this incident, PCU immediately launched an investigation into the nature and scope of the event including contacting the recipient of the information to alert them of the error and request that the document be destroyed. As part of the investigation, PCU conducted a review of the electronic document to identify those individuals whose information was included and determined that the document contained a limited number of image copies of deposited checks received by PCU. While PCU is not aware of any fraudulent activity or misuse of information as a result of this incident, PCU is providing potentially affected individuals with notice of this event because the document included name, member number, account number, and routing number for certain Maryland residents.

Notice to Maryland Residents

On or about May 8, 2023, PCU provided written notice of this incident to two (2) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, PCU moved quickly to investigate and respond to the incident, assess the security of the electronic documents, and identify potentially affected individuals. PCU is also working to implement additional safeguards and training to its employees.

Additionally, PCU is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their financial institution. PCU is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4637.

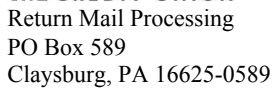
Very truly yours,

A handwritten signature in black ink, appearing to read 'Gregory Lederman', with a stylized, flowing script.

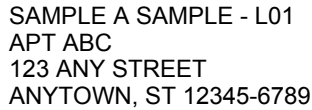
Gregory Lederman of
MULLEN COUGHLIN LLC

GCL/gcl
Enclosure

EXHIBIT A



J4120-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



Dear Sample A. Sample:

Provident Credit Union (“PCU”) is providing written notification of a recent event that may impact the security of some of your information. Although we have no indication that your information was subject to actual or attempted misuse, 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 or about September 23, 2022, PCU learned that an employee inadvertently sent an electronic document to a PCU member via the secure messaging portal that included check images that were deposited to other PCU member accounts. Upon learning of this incident, PCU immediately launched an investigation into the nature and scope of the event including contacting the recipient of the information to alert them of the error and request that the document be destroyed. While we are not aware of any fraudulent activity or misuse of information as a result of this incident, we are notifying you to provide you with information necessary to protect yourself, should you feel it is appropriate to do so.

What Information Was Involved? Upon review of the information, our investigation identified that the document contained a limited number of image copies of deposited checks received by PCU. We are notifying you because the investigation recently identified that the document included your [Extral]. Please note, this document did not contain other account information nor your Social Security number. Although we do not have evidence of actual or attempted misuse of your information as a result of this incident, PCU is providing this notice to you in an abundance of caution.

What We Are Doing. The confidentiality, privacy, and security of information we receive and in our care are among our highest priorities. Upon learning of the error, PCU moved quickly to investigate and respond to the event including a review of the event to identify and notify potentially impacted individuals. We are reviewing our policies and procedures and providing additional training to employees to further protect the security of information in our possession. We will also be notifying regulators, as required.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud over the next 12 to 24 months, to review your account statements, and monitor your credit reports for suspicious activity and promptly report any incidents of suspected identity theft. If you detect any suspicious activity on an account, you should promptly notify PCU or the financial institution with which the account is maintained. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Information*.



For More Information. If you have additional questions, please call (833) 468-0630 Monday–Friday from 9:00 a.m. to 11:00 p.m., and Saturday–Sunday from 11:00 a.m. to 8:00 p.m. Eastern Time (excluding major U.S. holidays). Please be prepared to provide engagement number B090393. You may also write to PCU at 303 Twin Dolphin Drive, Redwood City, CA 94065.

PCU values the trust you place in us to protect the privacy and security of your information. We apologize for any inconvenience or concern that this incident might cause you.

Sincerely,

Provident Credit Union

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

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

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

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

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

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission 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

0000001



theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.