

Via Email

August 20, 2024

Email: IDTheft@oag.state.md.us

Attorney General Anthony G. Brown
MD Office of Attorney General
200 St. Paul Place
Baltimore, MD 2120

Re: Data Incident Notification

Dear Attorney General Anthony Brown:

On behalf of our client, Patterson Federal Credit Union (“Lazarus Naturals”),¹ we are writing to provide information regarding a security incident involving customer personal information (the “Incident”).²

On February 29, 2024, PFCU discovered that personal information of its members, employees and/or vendors may have been accessible to an unauthorized actor(s) as a result of the Incident. Based on the investigation, it appears the Incident occurred at PFCU sometime on or around February 27, 2024.

Upon learning of this issue, PFCU immediately conducted a comprehensive investigation and communicated with its cyber security team. PFCU also contracted with third-party forensics experts to review the information potentially involved and by the end of April 2024, was able to confirm that member information may have been accessible to an unauthorized actor(s) as a result of the Incident. Given the nature of the data, PFCU performed a comprehensive review of the data to identify potentially impacted individuals and associated data elements.

PFCU has determined at this point in its investigation that personal information relating to certain members, employees and/or vendors may have been disclosed to the unauthorized actor(s) as a result of the Incident. The personal information may have included full name, address, Social Security number, date of birth, financial account information, and other financial documents.

To date, PFCU has identified 5151 individuals whose personal information may have been impacted by the Incident, of which 1 is believed to be a Maryland resident.

On August 8, 2024, PFCU commenced the notification process and begun mailing notices to affected individuals. Enclosed is the specimen letter being provided to affected individuals so they can take steps to

¹ PFCU’s corporate address is: 124 W.P. Malone Dr., Arkadelphia, AR 71923.

² Please note that by providing this letter PFCU is not agreeing to the jurisdiction of Maryland, or waiving its right to challenge jurisdiction in any subsequent actions. We are providing this notification as a courtesy.

minimize the risk that their information will be misused. PFCU will also be making credit monitoring and ID restoration protection services available at no cost to potentially affected persons. For persons who timely enroll, these services will be available for 12 months.

PFCU has taken numerous steps to protect the security of the personal information of the affected individuals. To help ensure an incident like this will not occur in the future, PFCU is reviewing its policies and procedures to make sure employees are reminded about best practices on data security.

If you require any additional information on this matter, please do not hesitate to contact me.

Very truly yours,

JACKSON LEWIS P.C.

Rob Yang

Robert Yang, Esq.

Encl.



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

Re: Notice of Data Security Incident

Dear <<Full Name>>:

At Patterson Federal Credit Union (“PFCU”), we value and respect the privacy of your information, which is why we are writing to inform you that on February 29, 2024, we discovered a data incident which may have impacted some member information (the “Incident”). While we are not aware of any misuse of your information, we are providing this notice to inform you of the Incident and to call your attention to 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 February 29, 2024, PFCU discovered that personal information of its members, employees and/or vendors may have been accessible to an unauthorized actor(s) as a result of the Incident. Based on the investigation, it appears the Incident occurred at PFCU sometime on or around February 27, 2024.

Upon learning of this issue, we immediately conducted a comprehensive investigation and communicated with our cyber security team. PFCU also contracted with third-party forensics experts to review the information potentially involved and by the end of April, was able to confirm that member information may have been accessible to an unauthorized actor(s) as a result of the Incident. Given the nature of the data, PFCU performed a comprehensive review of the data to identify potentially impacted individuals and associated data elements.

What Information Was Involved?

The following types of data may have included personal information such as your name, address, Social Security number, date of birth, financial account information, and other financial documents. Not all information was impacted for all individuals.

What We Are Doing.

PFCU takes this Incident and the security of your personal information very seriously. Upon learning of this incident, we launched an in-depth investigation to determine the scope of the Incident and identify those potentially affected. This included working with our information technology team and engaging third-party experts in an effort to ensure the Incident did not result in any additional exposure to personal information and taking steps to confirm the integrity of PFCU’s systems. We have also reported the Incident to law enforcement, the National Credit Union Administration to assist in our investigations and best protect from any incidents like this in the future. This communication was not delayed at the request of law enforcement. Additionally, because of the number of individuals potentially affected, PFCU will be providing notice of this incident to state authorities, consistent with state law. As an added precaution, we are also offering

complimentary access to identity monitoring, fraud consultation, and identity theft restoration services. If you wish to receive these services, activation instructions are below.

What You Can Do.

The attached sheet describes steps you can take to protect your identity and personal information. *While there is no evidence to suggest that any data involved in this incident has been misused*, out of an abundance of caution, PFCU recommends that impacted individuals regularly review their account statements and credit reports so they may be alerted to any incidents of fraud or identity theft.

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by <<Enrollment Deadline>>**.
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code: <<Activation Code>>**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by **<<Enrollment Deadline>>**. Be prepared to provide engagement number **<<Engagement Number>>** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-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, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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

For More Information.

PFCU apologizes for the inconvenience this may cause. We are committed to maintaining the security and privacy of personal information. We want you to be assured that we are taking steps to minimize the chances of a similar occurrence happening again. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call us at 1-888-596-5164, Monday through Friday from 8:00 a.m. to 8:00 p.m. central (excluding holidays).

Regards,

Shawn Cowart
CEO
Patterson Federal Credit Union

ADDITIONAL RECOMMENDED STEPS

We recommend you remain vigilant and consider taking the following steps to avoid identity theft, obtain additional information, and protect your personal information:

- Order Your Free Credit Report at www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information.
- Place a Fraud Alert on Your Credit File. A fraud alert helps protect you against an identity thief opening new credit in your name. With this alert, when a merchant checks your credit history when you apply for credit, the merchant will receive a notice that you may be a victim of identity theft and to take steps to verify your identity. You also have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can place a fraud alert or request a security freeze by contacting the credit bureaus. The credit bureaus may require that you provide proper identification prior to honoring your request.

Equifax	P.O. Box 105069 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.
- If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
- The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission ("FTC"). You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 1-877-IDTHEFT (1-877-438-4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.
- *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.
- *For New Mexico Residents:* You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more

information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to <http://consumersunion.org/pdf/security/securityNM.pdf>

- *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or <https://ag.ny.gov/internet/resource-center>; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or <https://dos.ny.gov/consumer-protection>.
- *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.