

MARY T. COSTIGAN
DIRECT DIAL: (908) 795-5135
EMAIL: MARY.COSTIGAN@JACKSONLEWIS.COM

March 26, 2024

VIA EMAIL: Idtheft@oag.state.md.us

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

Re: Data Security Incident

Dear Sir or Madam:

We represent U S #1364 Federal Credit Union (the “FCU”) located at 8400 Broadway, Merrillville, IN. Pursuant to Md. Code Ann. Comm. Law 14-3504, we are writing to notify you of a data incident.

On February 24, 2024, the FCU learned it was the victim of an external cyber security event. Upon discovering the attack, the FCU promptly took steps to contain, remediate and investigate the incident. As part of its investigation, the FCU engaged a cybersecurity forensic firm to perform a forensic investigation into the nature and scope of the incident including whether the incident impacted personally identifiable information. Based on its review of the investigation results, the FCU has determined the incident potentially impacted the personally identifiable information of ten (10) Maryland residents.

The FCU will be providing potentially affected individuals with written notice on or about March 27, 2024. The notice includes an offer to enroll in complimentary 12 month credit monitoring and identity restoration services. Please see attached letter.

The FCU continues to assess its security practices and will take steps, as necessary, to minimize the risk of a similar incident occurring in the future.

Please let us know if you have any questions.

Very truly yours,

JACKSON LEWIS P.C.

s/ Mary T. Costigan
Mary T. Costigan

MTC:dcw
Enclosures

4894-1129-5408, v. 1



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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

What Happened

We are writing to notify you that U S #1364 Federal Credit Union ("FCU") experienced a cybersecurity incident on or about February 22, 2024 (the "Incident"). With assistance from third-party experts, we took immediate steps to secure our systems, restore operations, and begin an investigation into the nature and scope of the Incident.

As part of our extensive investigation, we have been working diligently to identify any personally identifiable information ("PII") that may have been impacted. Based on our investigation, we have concluded that certain information located in our systems may have been subject to unauthorized access and acquisition during the Incident.

What Information Was Involved

This information may have included your name, address, <<b2b_text_1 (data elements)>>.

What We Are Doing

In response to this Incident and as part of our ongoing focus on cyber security, we have implemented additional safeguards including numerous firewall security enhancements. With the assistance of cyber security experts, we will continue to make additional improvements to ensure our I.T. systems are as secure as possible for the credit union and its members.

We are also offering you complimentary access to Experian IdentityWorksSM for 12 months. A credit card is not required to enroll 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 sign-up:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **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 ExtendCARETM:** 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.

While identity restoration assistance is immediately available to you, you must activate the fraud detection tools available through the Experian IdentityWorks complimentary 12 month membership.

To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll no later than 5:59pm CT on 06/11/2024 (Your code will not work after this date.)
- the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: <<Activation Code s_n>>

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 no later than 5:59pm CT on 06/11/2024. Be prepared to provide engagement number <<b2b_text_2 (engagement #)>> as proof of eligibility for the Identity Restoration services by Experian.

What You Can Do

In addition to enrolling in Experian IdentityWorksSM, you may wish to take certain precautionary measures listed at the end of this letter.

We apologize for any concern this Incident may cause you. If you have questions, please call our dedicated assistance line at (866) 495-4836, 8:00 am - 5:30 p.m. CT.

Sincerely,



Michelle Wilson

CEO

U S #1364 Federal Credit Union

8400 Broadway

Merrillville, IN 46410

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

** 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.

Additional Steps and Resources To Protect Your Personal Information

As with any data incident, we recommend remaining vigilant and taking any of the following steps to protect your personal information, as you deem appropriate:

1. Members can sign up for text or email alerts by logging into online banking and going to Additional Services > Alerts and Notifications. Here members can set up many different account alerts such as large withdrawal alerts, deposit alerts, as well as daily or weekly balance updates.
2. Contact the nationwide credit-reporting agencies as soon as possible to:

- Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You can contact one of the three agencies listed below and your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.
- Place a “security freeze” on your credit accounts. A security freeze prohibits a credit reporting agency from releasing any information from a consumer’s credit report without written authorization. Please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com).

To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies’ websites or over the phone, using the contact information below.

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

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, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver’s license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. 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.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

- Remove your name from mailing lists for pre-approved offers of credit for approximately six months.
- Receive and carefully review a free copy of your credit report by going to www.annualcreditreport.com.

<u>Equifax</u> P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	<u>Experian</u> P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	<u>TransUnion</u> Fraud Victim Assistance Dept. P.O. Box 2000 Chester, PA 19016-2000 https://www.transunion.com/fraud-alerts (800) 680-7289
--	--	--

3. Carefully review all bills and credit card statements for items that you did not contract for or purchase. Also review your bank account statements for unauthorized checks, purchases, or deductions. Even if you do not find suspicious activity initially, continue checking this information since identity thieves sometimes hold on to stolen personal information before using it.

4. Contact your local law enforcement or state attorney general if you suspect or know that you are the victim of identity theft.

You can also contact the Fraud Department of the FTC. The Fraud Department will collect your information and make it available to law enforcement agencies.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue
NW Washington, DC 20580
(877) 438-4338

5. Obtain additional information about identity theft.
 - *All US residents:* Obtain consumer assistance and educational materials on identity theft, privacy issues, and avoiding identity theft from the Federal Trade Commission ("FTC") at www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338.
 - *California Residents:* Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.
 - *Kentucky Residents:* Contact the Office of the Attorney General of Kentucky at 700 Capitol Avenue , Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.
 - *Iowa Residents:* Contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov.
 - *Maryland Residents:* Obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, marylandattorneygeneral.gov.
 - *New York Residents:* 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>.
 - *North Carolina Residents:* 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, 1-877566-7226, www.ncdoj.gov.
 - *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://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.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 https://www.ffnm.org/_kcms-doc/1254/38712/Credit-Freeze-Q-A-New-Mexico-Sept-2017.pdf.