Notice of Data Incident

We are writing to notify you that U S #1364 Federal Credit Union 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. Our investigation recently concluded and we have determined that during the Incident certain information located in our systems may have been subject to unauthorized access and acquisition. This information includes name, Social Security number, address, and account number. In the coming days we will be mailing you a letter, similar to this notice, which includes an opportunity to enroll in complimentary credit monitoring and related services.

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 our supplier's cyber security experts, we will continue to make additional improvements to ensure our systems are as secure as possible for the credit union and its members.

We apologize for any concern or inconvenience 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.

Additional Steps and Resources For Protecting 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. You 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. If you place a security freeze with one credit reporting agency, the freeze will not be shared with the other two credit reporting agencies and you will need to contact them separately. In your request, you must include: (i) your full name (including middle initial as well as Jr., Sr., II, III, etc.), address, Social Security number, and date of birth; (iii) if you have moved in the past five years, the address of each residence you lived at during that time period; (iv) proof of current address, such as a current utility bill or phone bill; and (v) a photocopy of a Social Security card, pay stub with SSN, W-2 or 1009 form.

- 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.

Equifax P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285
Experian P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742
TransUnion 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. Obtain consumer assistance and educational materials relating to 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.
5. Contact local law enforcement or your 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, which will collect your information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580