Nature of the Data Event

On or about June 27, 2024, First Commonwealth discovered unusual activity in its environment. Upon discovering this activity, First Commonwealth took steps to contain it and launched an investigation, aided by independent cybersecurity experts, to determine what happened and whether sensitive information may have been affected. The investigation determined that unauthorized actor acquired certain files and data stored within the systems on or around June 26, 2024. First Commonwealth then launched a comprehensive review of all potentially affected information to identify personal information that could have possibly been acquired. On July 1, 2024, First Commonwealth confirmed member personal information may have been involved in the incident. Out of an abundance of caution, First Commonwealth is providing notice to potentially impacted individuals whose address information could be identified following a diligent search.

The information that could have been subject to unauthorized access includes name, Social Security number, and account number.

Notice to Maine Residents

On or about August 2, 2024, First Commonwealth provided written notice of this incident to twenty-eight (28) Maine 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, First Commonwealth moved quickly to investigate and respond to the incident, confirm the security of First Commonwealth systems, and identify potentially affected individuals. Further, First Commonwealth notified law enforcement regarding the event. First Commonwealth is providing access to credit monitoring services for 12 (twelve) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, First Commonwealth 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 credit card company and/or bank. First Commonwealth 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.

First Commonwealth is providing written notice of this incident to relevant regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (310) 912-6183.

First Commonwealth
Federal Credit Union

P.O. Box 1907
Suwanee, GA 30024

<< First Name>> << Last Name>>
<<Address1>>, <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/fcfcu

August 2, 2024

Re: <<Variable Data 2>>

Dear << First Name>> << Last Name>>:

First Commonwealth Federal Credit Union ("First Commonwealth") is writing to notify you of a data security incident which may have impacted your personal information. First Commonwealth takes the privacy and security of your information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information.

What Happened? On June 27, 2024, we discovered unusual activity in our digital environment. Upon discovering this activity, we immediately took steps to contain it and launched an investigation, aided by independent cybersecurity experts, to determine what happened and whether sensitive information may have been affected. As a result of the investigation, we learned that an unauthorized actor acquired certain files and data stored within our systems on or around June 26, 2024. Upon learning this, we launched a comprehensive review of all potentially affected information to identify any personal information that could have possibly been acquired. That review remains ongoing at this time, but on July 1, 2024, we confirmed that a file likely containing your personal information may have been involved in the incident. Out of an abundance of caution, First Commonwealth is providing you this notice while our investigation is ongoing so that you can take any steps you feel are necessary to protect your information.

What Information was Involved? The information that could have been impacted by this incident includes your name, address, Social Security number, date of birth, or account number. At this time, we have no indication that your information was subject to actual or attempted misuse in connection with this incident.

What Are We Doing? First Commonwealth takes this incident and the security of information within our care very seriously. Upon discovery of this incident, First Commonwealth launched an in-depth investigation to determine the full nature and scope of the incident. As part of our ongoing commitment to the privacy of information in our care, we further strengthened our existing security policies and procedures as well as bolstered security to further protect against similar incidents in the future.

Additionally, First Commonwealth is providing you with information about steps that you can take to help protect your information and is offering identity theft protection services through IDX. The identity protection services include: <<12/24months>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

What You Can Do. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by scanning the QR code above, calling 1-888-461-3349, or going to https://response.idx.us/fcfcu and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is November 2, 2024.

We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and free credit reports to detect errors or suspicious activity. You can find more information about resources available to you to help protect your information from possible misuse in the enclosed *Steps You Can Take to Help Protect Your Information*.

We also encourage you to enable the security features and alerts available in the First Commonwealth Federal Credit Union Digital Banking application. These can be found in the Digital Banking User Guide located at www.firstcomcu.org/digitalbanking.

For More Information: If you have any questions or need assistance, we encourage you to contact our dedicated call center at 1-888-461-3349 between 9 am - 9 pm Eastern Time.

Sincerely,

First Commonwealth Federal Credit Union

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Request a Copy of Your Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Place a Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at https://www.annualcreditreport.com.

Put a Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission (FTC)
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.