Communication
FEDERAL CREDIT UNION
Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

XXXXXXXXX Name XXXXXXXXX
XXXXXXX ADDRESS 1 XXXXXXX
XXXXXXX ADDRESS 2 XXXXXXX
XXXXXX CITY XXXXXX, XX 99999-9999

August 12, 2024

NOTICE OF DATA BREACH

Dear Xxxxxxxxx Name Xxxxxxxxx:

For over 80 years, Communication Federal Credit Union has shared a commitment to serving our local communities and members. This includes a commitment to protect the information of our members and employees, and we have invested a great deal in measures designed to protect this information. Unfortunately, as is the case with many organizations regardless of their level of security, we recently experienced a cybersecurity incident.

We took immediate action to respond to and investigate the incident. While that process was ongoing, we posted information about this incident to our website on February 21, 2024. We are now reaching out to provide you additional information and an opportunity to enroll in free credit monitoring.

WHAT HAPPENED

We identified suspicious activity on our network systems on January 11, 2024, and we took immediate steps to secure our network systems and investigate the incident. We subsequently determined that an unauthorized third party gained access to a portion of our computer network that contained a number of files. Based on our investigation, we believe the unauthorized access occurred from December 31, 2023, to January 11, 2024. Once we identified the affected files, we promptly engaged a data-review firm to determine what information was contained in those files. We received the results of that review on July 15, 2024, and since then, we have been working to identify the correct addresses for the affected individuals.

WHAT INFORMATION WAS INVOLVED

Our investigation determined that some combination of the following types of information related to you was in the affected files: full name, date of birth, contact information, government identification (such as a driver's license or Social Security number), and financial information (such as a bank account and bank card numbers).

WHAT WE ARE DOING

We have security measures in place that allow us to take prompt action against attempted intrusions into our systems. Those measures reduced the scope of the unknown party's activity. We also hired third-party experts to address this situation, perform an investigation into the unauthorized activity, and further secure our systems to help protect the information we maintain.

WHAT YOU CAN DO

We encourage individuals to (1) remain vigilant for the next twelve to twenty-four months for unauthorized financial activity by reviewing account statements and free credit reports, (2) consider placing a fraud alert or security freeze on their credit file, and (3) immediately report any suspicious activity or suspected incidents of identity theft to the credit union and law enforcement. You can also find additional steps at www.IdentityTheft.gov/.

In addition, we are offering you a complimentary two-year membership to Experian's IdentityWorks. This product helps detect possible misuse of personal information. To register, please:

- Ensure that you **enroll by**: **11/7/2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: **XXXXXXXX CM Code XXXXXXXX**

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by **11/7/2024** and provide them engagement number [redacted]

FOR MORE INFORMATION

We have established a toll-free call center to support you and answer your questions. The call center can be reached at (888) 815-1120. Representatives are available at that number Monday through Friday 8:00 am to 6:00 pm Central Time. We appreciate your patience as we work through this process.

Sincerely,

Larry Shropshire
President/CEO
Communication Federal Credit Union
4141 NW Expressway, Suite 200
Oklahoma City, OK 73116
comfedcu.org

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – Review your account statements and free credit reports for the next twelve to twenty-four months for unauthorized financial activity.

- You should confirm that your financial institutions have the correct address on file for you and that all charges on your accounts are legitimate. If you discover errors or suspicious activity, you should immediately contact the financial institution and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit-reporting agencies. We recommend you do so and if the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a free, cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. Additional information is available at www.annualcreditreport.com.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Contact information for the three nationwide credit-reporting agencies:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, (800) 685-1111.
- Experian, PO Box 2104, Allen, TX 75013, www.experian.com, (888) 397-3742.
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, (800) 888-4213.

Federal Trade Commission

- If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC. Online guidance regarding steps you can take to protect against identity theft is available from the FTC at the website listed below.
- You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call (877)-ID-THEFT ((877) 438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

For Maryland Residents: the Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents: the North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents: the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; 1-800-771-7755; www.ag.ny.gov.

For Rhode Island Residents: the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and (401) 274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 3 Rhode Island residents impacted by this incident.

For Washington, D.C. Residents: the District of Columbia Attorney General may be contacted at: Office of the Attorney General, 400 6th Street, NW, Washington, D.C. 20001; (202) 727-3400; https://oag.dc.gov/.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including 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, and your rights pursuant to the FCRA, please visit:
https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

Communication
FEDERAL CREDIT UNION
Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

To the Parent or Guardian of:
XXXXXXXXX Name XXXXXXXXX
XXXXXXX ADDRESS 1 XXXXXXX
XXXXXXX ADDRESS 2 XXXXXXX
XXXXXX CITY XXXXXX, XX 99999-9999

August 12, 2024

NOTICE OF DATA BREACH

Dear Parent of Guardian of Xxxxxxxxx Name Xxxxxxxxx:

For over 80 years, Communication Federal Credit Union has shared a commitment to serving our local communities and members. This includes a commitment to protect the information of our members and employees, and we have invested a great deal in measures designed to protect this information. Unfortunately, as is the case with many organizations regardless of their level of security, we recently experienced a cybersecurity incident.

We took immediate action to respond to and investigate the incident. While that process was ongoing, we posted information about this incident to our website on February 21, 2024. We are now reaching out to provide you additional information and an opportunity to enroll your child in free credit monitoring.

WHAT HAPPENED

We identified suspicious activity on our network systems on January 11, 2024, and we took immediate steps to secure our network systems and investigate the incident. We subsequently determined that an unauthorized third party gained access to a portion of our computer network that contained a number of files. Based on our investigation, we believe the unauthorized access occurred from December 31, 2023, to January 11, 2024. Once we identified the affected files, we promptly engaged a data-review firm to determine what information was contained in those files. We received the results of that review on July 15, 2024, and since then, we have been working to identify the correct addresses for the affected individuals.

WHAT INFORMATION WAS INVOLVED

Our investigation determined that some combination of the following types of information related to your child was in the affected files: full name, date of birth, contact information, government identification (such as a driver's license or Social Security number), and financial information (such as a bank account and bank card numbers).

WHAT WE ARE DOING

We have security measures in place that allow us to take prompt action against attempted intrusions into our systems. Those measures reduced the scope of the unknown party's activity. We also hired third-party experts to address this situation, perform an investigation into the unauthorized activity, and further secure our systems to help protect the information we maintain.

WHAT YOU CAN DO

We encourage individuals to (1) remain vigilant for the next twelve to twenty-four months for unauthorized financial activity by reviewing account statements and free credit reports, (2) consider placing a fraud alert or security freeze on their credit file, and (3) immediately report any suspicious activity or suspected incidents of identity theft to the credit union and law enforcement. You can also find additional steps at www.IdentityTheft.gov/.

In addition, we are offering your child a complimentary two-year membership to Experian's IdentityWorks Minor Plus. This product helps detect possible misuse of personal information. To register, please:

- Ensure that you **enroll by**: **11/7/2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/minorplus
- Provide your **activation code**: **XXXXXXXX CM Code XXXXXXXX**

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by **11/7/2024** and provide them engagement number [redacted].

FOR MORE INFORMATION

We have established a toll-free call center to support you and answer your questions. The call center can be reached at (888) 815-1120. Representatives are available at that number Monday through Friday 8:00 am to 6:00 pm Central Time. We appreciate your patience as we work through this process.

Sincerely,

Larry Shropshire
President/CEO
Communication Federal Credit Union
4141 NW Expressway, Suite 200
Oklahoma City, OK 73116
comfedcu.org

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – Review your account statements and free credit reports for the next twelve to twenty-four months for unauthorized financial activity.

- You should confirm that your financial institutions have the correct address on file for you and that all charges on your accounts are legitimate. If you discover errors or suspicious activity, you should immediately contact the financial institution and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit-reporting agencies. We recommend you do so and if the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a free, cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. Additional information is available at www.annualcreditreport.com.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission. There is no fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Contact information for the three nationwide credit-reporting agencies:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, (800) 685-1111.
- Experian, PO Box 2104, Allen, TX 75013, www.experian.com, (888) 397-3742.
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, (800) 888-4213.

Federal Trade Commission

- If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC. Online guidance regarding steps you can take to protect against identity theft is available from the FTC at the website listed below.
- You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call (877)-ID-THEFT ((877) 438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

For Maryland Residents: the Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents: the North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents: the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; 1-800-771-7755; www.ag.ny.gov.

For Rhode Island Residents: the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and (401) 274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 3 Rhode Island residents impacted by this incident.

For Washington, D.C. Residents: the District of Columbia Attorney General may be contacted at: Office of the Attorney General, 400 6th Street, NW, Washington, D.C. 20001; (202) 727-3400; https://oag.dc.gov/.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including 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, and your rights pursuant to the FCRA, please visit:
https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.