



Robert Bender
Constangy, Brooks, Smith & Prophete, LLP
bbender@constangy.com
445-308-1588
Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

June 6, 2025

VIA ONLINE SUBMISSION

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509

Re: Notification of Data Security Incident

To Whom It May Concern,

Constangy, Brooks, Smith & Prophete, LLP represents LG&W Federal Credit Union located at 1616 Whitten Road Memphis, TN 38134 in conjunction with their response to a recent data event involving information for a Nebraska resident. The purpose of this letter is to notify you of the incident and to provide a summary of the incident and response. LG&W Federal Credit Union does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data security notification statute, or personal jurisdiction.

1. Nature of the Security Incident

In November 2024, LG&W Federal Credit Union identified suspicious activity within its network. LG&W Federal Credit Union immediately investigated with assistance from cybersecurity experts. The investigation determined unauthorized individuals accessed our network between October 30, 2024 and November 6, 2024 and accessed some files on the network during that window. LG&W Federal Credit Union undertook a comprehensive review of those files to determine the specific information present in the files. After completing the review, LG&W Federal Credit Union reviewed records to confirm available address information on so it could notify these individuals and completed the process on June 3, 2025.

2. Number of Affected Nebraska Residents & Information Involved

The incident involved information for approximately one Nebraska resident. The information involved in the incident for the Nebraska resident includes name, Social Security number, and financial account information.

3. Notification to Affected Individuals

On June 6, 2025, LG&W Federal Credit Union notified one Nebraska resident by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers the opportunity to enroll in complimentary identity protection services including credit monitoring, financial tracking, \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter is enclosed.

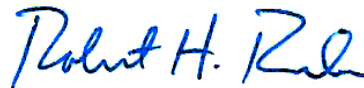
4. Measures Taken to Address the Incident

Upon discovering this incident, LG&W Federal Credit Union conducted an immediate and comprehensive investigation to confirm the scope of the event to secure its network and to notify affected individuals. LG&W Federal Credit Union also reported the event to the FBI and to the National Credit Union Administration. LG&W Federal Credit Union established a toll-free call center to answer questions about the incident and to address related concerns. LG&W Federal Credit Union continues to review policies and procedures and so it can implement additional measures as appropriate.

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at bbender@constangy.com or 445-308-1588.

Sincerely,



Robert Bender
Partner, Constangy Cyber Team

Encl.: Sample Notification Letter



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>>

Subject: Notice of Data Event

Dear <<Full Name>>:

LG&W Federal Credit Union takes the privacy and security of all information within its possession very seriously. We are informing you of a recent data security incident that may have involved your personal information. This letter contains information regarding the incident, our response, and steps that you can take to help protect your personal information, including enrolling in complimentary identity protection services.

What Happened. On January 30, 2025, LG&W FCU first determined some of your information was involved in the incident. In November 2024, we identified suspicious network activity that disrupted the credit union's network. We took immediate steps to secure the network and implemented emergency measures to minimize impact to credit union operations. We also investigated the event with support from independent cybersecurity specialists to assist with the process. The investigation determined some files were acquired without authorization around November 6, 2024. LG&W FCU then undertook a comprehensive review of those files that completed on January 30, 2025. After completing the review, we reconciled the information with available records so we could notify individuals. We are notifying you because we learned some of your personal information was contained within the data that was accessible to the unauthorized individuals.

What Information Was Involved. The information may have included your name, Social Security number, and financial account number. We have no evidence of any identity theft or fraud rising from the incident.

What We Are Doing. As soon as LG&W FCU discovered suspected activity, we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. LG&W FCU notified the FBI and will cooperate with any resulting investigation. LG&W FCU is also offering you complimentary identity protection services through CyEx, a leader in consumer identity protection. These services include access to credit monitoring¹, financial tracking, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll in these services is <<Enrollment Deadline>>. To enroll, please visit app.financialshield.com/enrollment/activate/lgwfcu and do the following:

1. Enter your unique Activation Code <<Activation Code>>

¹ To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

2. Click “Redeem Code”

3. Follow the prompts to create your account

If you need assistance with the enrollment process or have questions regarding Financial Shield, please call Financial Shield directly at 1.866.622.9303.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, from any source, over the next 12 to 24 months, including by reviewing account statements and monitoring free credit reports for suspicious activity and errors. You can also enroll in the complementary services offered to you by using the instructions included with this letter.

For More Information. Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call 888-408-3545 Monday through Friday from 9 a.m. to 9 p.m. (excluding holidays). We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

LG&W Federal Credit Union

Steps You Can Take to Help Protect Your Personal 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.

Copy of 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 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

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 www.annualcreditreport.com.

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.

Residents of the below states can obtain additional information about the steps you can take to avoid identity theft:

- **Maryland residents:** Maryland Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; <https://www.marylandattorneygeneral.gov> or 1-410-528-8662 or 1-888-743-0023.
- **Massachusetts residents:** Under Massachusetts law, you have the right to obtain any police report that has been filed.
- **New York residents:** Office of the New York Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov>; or 1-800-771-7755.
- **North Carolina residents:** North Carolina Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; <https://ncdoj.gov>; and toll-free at (877) 566-7226 or (919) 716-6000.

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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.