



Lauren Godfrey, Partner
Cybersecurity & Data Privacy Team
322 North Shore Drive, Building 1B, Suite 200
Pittsburgh, PA 15212
lgodfrey@constangy.com
Mobile: 973.462.9521
www.constangy.com

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

October 14, 2025

VIA ONLINE SUBMISSION

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capital
Lincoln, NE 68509
Tel: 402-471-2683

Re: Notification of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents FSA Marketing Systems, Inc. (“FSA”) in conjunction with their response to a recent data event involving information for Nebraska residents. The purpose of this letter is to notify you of the incident in accordance with Nebraska’s data breach notification statute. FSA does not waive any rights or defenses regarding the applicability of Nebraska law or personal jurisdiction.

1. Nature of the Security Incident

On or about February 17, 2025, FSA was alerted to suspicious activity related to its computer network, promptly took steps to secure its environment and immediately initiated an investigation of the matter. FSA engaged independent cybersecurity experts to assist with this process. The investigation determined that certain files may have been acquired without authorization between January 11 and 27, 2025. FSA engaged a third-party vendor to complete a comprehensive and thorough review of the data potentially involved to identify what personal information may have been impacted and to whom it belonged. FSA then identified and confirmed contact information to notify the potentially impacted individuals. This process was completed on October 8, 2025.

2. Number of Affected Nebraska Residents & Information Involved

The incident involved information for approximately 2 Nebraska residents. The information involved in the incident for Nebraska residents includes names, driver’s license or state ID numbers, and Social Security numbers.

3. Notification to Affected Individuals

On or around October 14, 2025, FSA notified 2 Nebraska residents 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 12 months of credit monitoring, dark web monitoring, \$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, FSA conducted an immediate and comprehensive investigation to confirm the scope of the event to secure its network and to notify affected individuals. FSA established a toll-free call center through IDX to answer questions about the incident and to address related concerns. FSA 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 lgodfrey@constangy.com or 973.462.9521.

Sincerely,

Lauren D. Godfrey

Lauren Godfrey
Partner, Constangy Cyber Team

Encl.: Sample Notification Letter



Return Mail Processing Center:
P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>

Enrollment Code: <<XXXXXXXXXX>>
Enrollment Deadline: January 14, 2026

To Enroll, Scan the QR Code Below:



Or Visit:
<https://app.idx.us/account-creation/protect>

October 14, 2025

Subject: Notice of Data <<Variable Text 1: Security Incident / Breach>>

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

FSA Marketing Systems Inc. ("FSA") is writing to inform you of a recent data security incident that may have affected your information. We take the privacy and security of all information within our possession seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

What Happened. On or about February 17, 2025, we experienced a network disruption and promptly took steps to secure our environment and initiated an investigation of the matter. We engaged independent cybersecurity experts to assist with the process. As a result of the investigation, we determined that certain files may have been acquired without authorization between January 11 and 27, 2025. We then completed a comprehensive and thorough review of the data potentially involved to identify what personal information may have been impacted and to whom it belonged. Following that review, we worked to obtain and confirm the contact information necessary to send you this letter which was completed on September 28, 2025. Please note that we have no evidence of the misuse, or attempted misuse, of any potentially impacted information.

What Information Was Involved. The information varied per individual but may have included your name, Social Security number, and Driver's License or State ID number.

What We Are Doing. As soon as we discovered this incident, we took the steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and will cooperate with any resulting investigation.

Although we have no evidence of the misuse of any information as a result of this incident, we are also offering you complimentary identity protection services through IDX a leader in consumer identity protection. These services include <<12 / 24>> months of credit monitoring¹, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll in these services is January 14, 2026. To enroll services at no charge, please log on to <https://app.idx.us/account-creation/protect> and follow the instructions provided. When prompted please provide the following unique code to receive services: <<Enrollment Code>>.

What You Can Do. You can follow the recommendations on the following page to help protect your information. You can also enroll in the complementary services offered to you through IDX by using the enrollment code provided above. You can also remain vigilant by reviewing account statements and monitoring free credit reports.

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.

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 (833) 274-4431 Monday through Friday from 9 am – 9 pm Eastern Time, excluding U.S. 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,

FSA Marketing Systems, Inc.
50 W Big Beaver Rd., Suite 500
Troy, MI 48084

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 (the “FTC”).

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 2000
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.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

Oregon Attorney General

1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General

1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General

The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400
[#] Rhode Island residents were affected by the incident.

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

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.