



Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

May 19, 2022

VIA ELECTRONIC MAIL

Attorney General Frosh
Office of the Attorney General
Attn: Security Incident Notification
200 St. Paul Place
Baltimore, MD 21202

Re: **Notification of Data Security Incident**

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Kanza Cooperative Association ("Kanza"), a farmer's cooperative located in Iuka, Kansas, in connection with a recent data security incident described in greater detail below.

1. Nature of the Security Incident

On September 15, 2021, Kanza discovered unusual activity in their computer network. Upon discovery, Kanza took immediate steps to secure its systems. In addition, Kanza retained outside cybersecurity experts to conduct an investigation to determine the source and scope of the incident. The forensic investigation revealed that an unauthorized third party gained access to Kanza's network on September 9, 2021. Kanza confirmed that some sensitive, personal information was potentially impacted. Thereafter, Kanza worked to identify address information for the impacted individuals and prepared notification materials.

2. Type of Information and Number of Maryland Residents Involved

A total of 4 residents of Maryland were notified about this incident. The information involved may include individuals names, Social Security numbers, bank account information, financial account numbers, payment card numbers, payment card CVV/expiration dates, and PIN/Access Code/Passwords.

Notification letters were mailed via USPS First Class Mail on May 18, 2022 providing impacted with information about the incident, offering complimentary identity protection services, and providing additional steps they can take to protect their personal information. A sample copy of that letter is included with this notice.

3. Measures Taken to Address the Incident

Upon learning of this incident, Kanza engaged a computer forensics firm to conduct an investigation into the incident and has taken steps to secure their network. In addition, Kanza has notified the potentially impacted individuals and provided them with information about steps they can take to help protect their personal information as well as offering complimentary identity protection services, 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

4. Contact Information

Kanza is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Lindsay Nickle at Lindsay.Nickle@lewisbrisbois.com.

Sincerely,



Lindsay Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP



P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:

1-833-774-2185

Or Visit:

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

Enrollment Code:

<<XXXXXXXXXX>>

<<First Name>> <<Last Name>>

<<Address 1>> <<Address>>

<<City>>, <<State>> <<Zip>>

May 18, 2022

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a data security incident that involved your personal information. 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. At Kanza Cooperative Association ("Kanza"), we take the privacy and security of our member information very seriously. This is why I am notifying you about the incident, offering you credit monitoring and identity monitoring services, and informing you about steps you can take to help protect your personal information.

What Happened? On September 15, 2021, Kanza learned about suspicious activity in our computer network. Upon discovery, we took immediate steps to secure our systems. In addition, we retained outside cybersecurity experts to conduct an investigation to determine the source and scope of the incident. The forensic investigation revealed that an unauthorized third party gained access to our network on September 9, 2021. Based on the findings from the investigation, we reviewed the affected systems to determine whether personal information was impacted as a result of the incident. We also took steps to confirm which individuals may have been impacted. We determined that your personal information may have been impacted by this incident.

What Information Was Involved? The information involved was your name, <<variable data 1>>.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We also notified the Federal Bureau of Investigation and will cooperate with any resulting investigation. In addition, we are providing you information about steps you can take to help protect your personal information. We are offering you free identity monitoring and recovery services for <<12/24 months>> through IDX, a data breach and recovery services expert, as described below.

What You Can Do: You can follow the recommendations included with this letter regarding steps you can take to protect your personal information. In addition, we encourage you to enroll in the complimentary credit monitoring and identity monitoring services we are offering through IDX to protect your personal information. To enroll, please visit <https://app.idx.us/account-creation/protect> or call 1-833-774-2185 and give them the enrollment code provided above. Your <<12/24 months>> of services will include the following:

- **Single Bureau Credit Monitoring** – will alert you in the event there is any change in your credit file.
- **Insurance** – a \$1,000,000 reimbursement insurance policy.
- **CyberScan Monitoring** – will alert you to trading or selling of your personal information on underground websites and chat rooms.
- **Identity Theft Recovery Service** – will provide professional help in the event you experience any kind of identity theft, either financial or non-financial. A professional Recovery Advocate will help you with fraud alerts, reviewing credit reports and resolving any incident of identity theft.

To receive the services offered, you must be an individual 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. Additional information describing your services is included with this letter. Please note you must enroll by August 18, 2022.

For More Information: If you have any questions about this letter or would like assistance enrolling in the services offered, please call 1-833-774-2185. IDX representatives are available Monday through Friday from 8 am - 8 pm Central Time. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

The security of your information is a top priority at Kanza, and we are committed to safeguarding your data. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Bruce Krehbiel", with a stylized, looping flourish at the end.

Bruce Krehbiel
CEO
Kanza Cooperative Association

Steps You Can Take to 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 (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 <http://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 <http://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, 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>.