BOK FINANCIAL

One Williams Center, 16th floor
Tulsa, OK 74172

bokfinancial.com

[CLIENT NAME]
[ADDRESS]
[CITY], [STATE] [ZIPCODE]
NOVEMBER 21, 2025

NOTICE OF CYBERSECURITY INCIDENT AT LINEDATA SERVICES, INC.

Dear [FIRST NAME] [LAST NAME]:

At BOKF NA ("BOKF"), we place a high value on earning your trust, earning your business, and respecting your privacy and the privacy of your information. This is why, as a precautionary measure, we are writing to let you know about a data security incident with one of our vendors that involves your personal information. While we are unaware of any attempted or actual misuse of any information involved in this incident, we are providing you with information about the incident and steps you can take to protect yourself, should you feel it necessary.

WHAT HAPPENED?

On August 12, 2025, BOKF was notified that Linedata Services Inc. ("Linedata") was the victim of a cybersecurity incident detected the day before. Linedata is a global solutions and outsourcing services provider to the investment management and credit finance industries, and Linedata provides services for various lines of business among BOKF, its subsidiaries, and affiliates.

In August, BOKF was not aware that any of our clients' personal data was involved in the incident. Linedata reported that it was actively working with cybersecurity experts to resolve the issue, which involved malicious encryption of data hosted on a specific domain within its asset management business line. However, on October 23, we determined that your personal information was located within a dataset that could have been improperly accessed in the Linedata incident.

WHAT INFORMATION WAS INVOLVED?

The data that could have been accessed included your name and social security number. At this time, we have no indication that your information has been misused.

WHAT WE ARE DOING

BOKF values your privacy and deeply regrets that this incident occurred. BOKF is closely monitoring communications with Linedata for updates on its forensic investigation. Linedata is

working with relevant law enforcement and cybersecurity experts to address the issue. BOKF will notify you of significant developments that affect your personal data.

WHAT YOU CAN DO

Please also review the attachment to this letter (*Steps You Can Take to Further Protect Your Information*) for further information on steps you can take to protect your information, and how to receive free credit monitoring services for one (1) year.

BOKF has also compiled a list of general tips to help safeguard financial and identifying information on its website at https://www.bokfinancial.com/legal-and-privacy/preventing-account-fraud. If you notice irregular activity with respect to your account(s), please notify bokonlinefraud@bokf.com.

FOR MORE INFORMATION

For further information, please contact your account manager, or call 918-879-7082, Monday – Friday, 8am – 5pm Central Time.

Sincerely,

BOK Financial

Steps You Can Take to Further Protect Your Information

BOKF has compiled a list of general tips to help safeguard financial and identifying information on its website at https://www.bokfinancial.com/legal-and-privacy/preventing-account-fraud.

You may wish to consider doing the following:

- **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, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you 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 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 can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action. Or, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(866) 349-5191	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 2002	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

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 90 days. 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 above. Visit www.annualcreditreport.com for more information.

- **Credit Report Monitoring**

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for **12 months** from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive

fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: <CODE>

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of *Identity Theft – A Recovery Plan*, a guide from the FTC to help guard against and deal with identity theft, can be found at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

OTHER IMPORTANT INFORMATION

- **Security Freeze**

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request or to remove a security freeze.