EXHIBIT 1

By providing this notice, Financial Foundations does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

Financial Foundations became aware that an unauthorized party accessed one of its information system. It immediately took steps to secure the system and launched an investigation with support from its Broker/Dealer, a third-party IT vendor, and a third-party cybersecurity/forensic specialist. The investigation determined that the unauthorized party gained access to the information system, which was monitored by a third-party IT company at the time. It is important to note that business operations were unaffected, Financial Foundations' current network remains secure, no client data was lost or altered, and client accounts and investments were unaffected. Because the incident was limited, there was no disruption to Financial Foundations' business operations. In an abundance of caution, Financial Foundations began a diligent and comprehensive review process to determine all personal information that resided on the server and thus may have been accessed by the unauthorized party. This comprehensive review took time, and Financial Foundations prioritized accuracy to ensure it provided correct and specific information once the scope became clear. This review has now been completed, and Financial Foundations is notifying all potentially impacted individuals.

The information that could have been subject to unauthorized access includes name, Social Security number or Individual Taxpayer Identification number, and financial account number without access information.

Notice to Nebraska Resident

On May 8, 2026, Financial Foundations began providing written notice of this incident to one (1) Nebraska resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Financial Foundations moved quickly to investigate and respond to the incident, assess the security of Financial Foundations systems, and identify potentially affected individuals. Financial Foundations is also working to implement additional safeguards and training to its employees. Financial Foundations is providing access to credit monitoring services for twelve (12) months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Importantly, prior to the event, Financial Foundations implemented additional security measures within their network and completed a review of its policies and procedures to further secure the information in its systems. These efforts included moving its data from a physical server to Microsoft Cloud, with Multi-Factor-Authentication. The data now resides on Microsoft Cloud with these enhanced protections in place.

Additionally, Financial Foundations is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Financial Foundations is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state attorney general, and law enforcement to report attempted or actual identity theft and fraud.

Financial Foundations is providing written notice of this incident to relevant state regulators, as necessary.

EXHIBIT A

FINANCIAL FOUNDATIONS
Complicated Made Simple®

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

SCAN TO ENROLL

<<Date>> (Format: Month Day, Year)

<<b2b_text_1 (Re: Notice of [Security Incident / Data Breach])>>

Dear <<First_name>> <<Last_name>>:

Financial Foundations, Inc. ("Financial Foundations") is writing to inform you of a recent incident that may affect the security of some of your information. We are providing you with information about the incident, actions we have taken, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? Financial Foundations became aware that an unauthorized party accessed one of our information systems We immediately took steps to secure the system and launched an investigation with support from our Broker/Dealer, a third-party IT vendor, and a third-party cybersecurity/forensic specialist.

Our investigation determined that the unauthorized party gained access to the information system, which was monitored by a third-party IT company at the time. It is important to note that business operations were unaffected, our current network remains secure, no client data was lost or altered, and client accounts and investments were unaffected. Because the incident was limited, there was no disruption to our business operations.

In an abundance of caution, we began a diligent and comprehensive review process to determine all personal information that resided on the server and thus may have been accessed by the unauthorized party. This comprehensive review took time, and we prioritized accuracy to ensure we provided correct and specific information once the scope became clear. This review has now been completed, and Financial Foundations is notifying all potentially impacted individuals.

What Information Was Involved? The investigation determined the following types of information were present in the impacted systems: your We currently have no evidence that any information related to this incident has been used to commit identity theft or fraud.

What We Are Doing. This incident involved a legacy information system that has since been permanently taken offline. The privacy and security of client information is one of our top priorities. Before this incident, we had made the proactive decision to move data from a physical server to Microsoft Cloud, which offers enhanced security monitoring and scalability. The data now resides on Microsoft Cloud with these enhanced protections in place.

Although we have no evidence that any information has been used to commit identity theft or fraud, we are, as an added precaution, offering you <<ServiceTerminMonths>> months of credit monitoring and identity restoration services to you at no cost through Kroll. Enrollment instructions are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You May Take to Help Protect Personal Information* for useful information on what you can do to better protect against possible misuse of your information. You may also enroll in the free credit monitoring services we have provided for you.

For More Information. If you have additional questions regarding credit monitoring and identity restoration services enrollment, you may call their call center at (844) 576-2703 (toll free), Monday through Friday, 8:00 am to 5:30 pm Central Time, excluding U.S. holidays. You may write to Financial Foundations at 2 Park Central Drive, Suite 310, Southborough, MA 01772 or call 508-620-1000.

Sincerely,

Nicholas Cosentino, CEO and President
Financial Foundations Inc.

Steps You May Take to Help Protect Personal Information

Enroll in Credit Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<ServiceTerminMonths>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until ***<<b2b_text_6 (activation deadline)>>*** *to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.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 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this incident. There are approximately [#] Rhode Island residents that may be impacted by this incident.