NICHOLAS H. SAFFORD & CO., INC.

INVESTMENT COUNSEL • PRIVATE TRUSTEES

9 CLEAVES STREET ROCKPORT, MA 01966

TELEPHONE: 978 546·2462 FACSIMILE: 978 546·2307

<<MemberFirstName>><<MemberMiddleName>><<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

NOTICE OF SECURITY INCIDENT

Dear <<MemberFirstName>><<MemberLastName>>,

Nicholas H. Safford & Co., Inc. ("***we***," "***us***," or "***our***") is writing to provide notice of a recent security incident that we experienced that may have exposed your personal information. This notice will provide you with information about the event, our response, and additional measures you can take to help protect your information.

WHAT HAPPENED: We recently became aware of unauthorized access into a limited subset of our internal electronic systems that occurred between January 30, 2026 and March 12, 2026 (the "***Access Period***"). When the unauthorized access was discovered, it was immediately terminated. We promptly took steps to secure our systems and initiated a comprehensive investigation which revealed that the unauthorized access was limited to a single employee's email account.

We have taken steps to fully understand the scope of the security incident and what information may have been exposed: we have consulted with legal counsel, contacted law enforcement, and engaged a cyber forensics firm to conduct a thorough investigation.

WHAT INFORMATION WAS INVOLVED: Based on our investigation, it is possible that some of your personal data may have been exposed during the Access Period, including the following: *[Full Name, Date of Birth, Partial or full Social Security Number or Employer or Taxpayer Identification Number, Account Number, [Government-Issued Driver's License, Passport or Identification Number], Mother's Maiden Name]*.

Although your personal information as identified above may have been exposed for the time period identified above, based on our investigation we are aware of no evidence that your personal information has been acquired, used, or compromised in any way.

WHAT WE ARE DOING: Your confidentiality, privacy and security of personal information is of utmost importance to us. When we learned of this incident, we promptly began working with legal and forensic cyber specialists to help us determine the scope of the impact and the relevant sensitive data that may have been exposed. We are also taking forward-looking measures to improve our security, such as engaging with an additional cybersecurity vendor and reviewing our internal policies and procedures.

Additionally, to help relieve concerns following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 24 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. See the enclosed *Steps You Can Take to Help Protect Personal Information* for information on enrollment, which we encourage you to do, as we cannot do so on your behalf.

WHAT YOU CAN DO: We recommend that you review your banking and credit activity as soon as possible to determine if there are any discrepancies listed or any unusual activity (such as unauthorized charges, withdrawals, account openings or inquiries from creditors you did not initiate). You should continue to monitor your accounts and statements with financial institutions for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should immediately contact us or the relevant financial institution, or a credit agency, to report such suspicious activity. Please also review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains information on what you can do to safeguard your information.

As always, we are here to answer your questions or discuss your concerns, so please contact us if you have additional questions. We can be reached by phone at 978-546-2462, by email to john@saffords.com or quinn@saffords.com, or via mail to our office at 9 Cleaves St, Rockport MA, 01966.

Keeping your information secure is and has always been of the utmost importance to us. We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

John Safford
President

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

ENROLL IN MONITORING SERVICE: 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 24 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/redeem to activate and take advantage of your identity monitoring services.

You have until **July 8, 2026** to activate your identity monitoring services. Your Activation Code will not work after this date.

Provide Your Activation Code: **<<Activation Code>>** and Your Verification ID: **SF-013836**

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

MONITOR YOUR ACCOUNTS:

We recommend that you periodically obtain credit reports from each nationwide credit reporting company and that you have information relating to fraudulent transactions deleted. To obtain a copy of your credit report, you can contact the three major credit reporting agencies as follows:

- Equifax: 1-800-685-1111, Equifax.com/personal/credit-report-services
- Experian: 1-888-397-3742, Experian.com/help
- TransUnion 1-888-909-8872, TransUnion.com/credit-help

Federal law gives you the right to obtain a free copy of your credit report every 12 months from each of the three nationwide credit bureaus. In addition, the three bureaus have permanently extended a program that lets you check your credit report from each once a week for free at AnnualCreditReport.com. More information regarding how to obtain free credit reports can be found at:

https://consumer.ftc.gov/articles/free-credit-reports#How%20To%20Get%20Your%20Free%20Credit%20Reports.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You can also place a security freeze and fraud alert in your credit reports. Freezes prevent new credit accounts from being opened in your name. Fraud alerts make lenders verify your identity

before they grant new credit in your name and put creditors on notice that you may be a victim of fraud, including identity theft. Further information on different types of fraud alerts, including how to place a fraud alert with Equifax, Experian, and TransUnion is provided at: https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts.

We encourage you to report any incidents of identity theft to the Federal Trade Commission. You may obtain government information about identity theft and report suspected incidents of identity theft at https://www.ftc.gov/news-events/topics/identity-theft/report-identity-theft and https://www.identitytheft.gov/. Further guidance from *usa.gov* regarding steps that you can take to protect against identity theft can be found at https://www.usa.gov/identity-theft.

ADDITIONAL INFORMATION:

You have the right to obtain a police report. If you believe you are the victim of identity theft, or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

As a Massachusetts resident, you may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, (617) 727-8400, www.mass.gov/ago/contact-us.html. You may also contact the Director of the Office of Consumer Affairs and Business Regulation, 10 Park Plaza, Suite 5170, Boston, MA 02116, (617) 973-8787.