Navigate360
c/o HaystackID Return mail processing

<<Address 1>> | <<City, State ZIP>>

Via First-Class Mail

<FirstName> <LastName>
<Address1>
<Address2>
<City> <State> <PostalCode+4>
<Country>

<<Date>>

Re: Notice of Data Security Incident <<Header>>

Dear <<FirstName>> <<LastName>>,

Navigate360 is committed to protecting the privacy and confidentiality of your information. We are writing to inform you that we recently identified and addressed an incident involving some of your information. This notice explains the incident, the measures we have taken in response, and some additional steps that you can consider taking.

What Happened?

On or about March 18, 2026, Navigate360 became aware of suspicious activity on one of its systems. Navigate360 immediately instituted mitigation measures to minimize any disruption while also investigating the activity. Navigate360 launched an investigation into the nature and scope of the incident with the assistance of a leading cybersecurity firm, which determined that an unauthorized third party accessed one of our systems and obtained copies of some data between November 21, 2025 to March 5, 2026. Navigate360 has engaged a data mining firm to undertake a detailed review of this data to determine the incident's impact and has determined that some of these files may have contained your information.

What Information was Involved?

The personal information that may have been subject to unauthorized access includes name and the following data elements: <<data elements>>. We have no evidence of misuse of any personal information for fraud or identity theft. Please note the information impacted varies for each potentially impacted individual.

What We Are Doing.

Upon discovery of this incident, Navigate360 immediately instituted mitigation measures. Navigate360 promptly implemented additional and enhanced safeguards and enlisted the support of a leading cybersecurity firm to enhance the security of our network, systems, and data. Navigate360 also launched a comprehensive investigation, identified individuals who may have been affected, reported the incident to law enforcement, and notified regulatory bodies.

As an added precaution, we are offering <<CM Duration>> months of complimentary credit monitoring and identity protection services through HaystackID, a company specializing in these services. Instructions for how to enroll in these services are below.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to the following and follow the instructions provided: **www.equifax.com/activate**.

When prompted please provide the following activation code to receive services: **<<Activation Code>>**.

In order for you to receive the monitoring services described above, you must enroll within ninety (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.

What You Can Do.

We encourage you to enroll in the complimentary credit monitoring that we are offering to you at no cost. Additionally, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. You can find more information on steps to protect yourself against identity theft identity theft in the enclosed *Additional Resources to Help Protect Your Information* sheet.

For More Information.

If you have any questions or concerns not addressed in this letter, please call 833-966-1754 (toll free) Monday through Friday, during the hours of 9:00 a.m. and 9:00 p.m. Eastern Standard Time (excluding U.S. national holidays). Please have this letter ready if you call.

Navigate360 sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Navigate360

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative, you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. You can obtain further information on how to file such a complaint by way of the contact information listed above.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state, and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

California and Wyoming residents are advised that notification was not delayed due to a law enforcement investigation.

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Kentucky residents can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for Kentucky, at 1024 Capital Center Drive, Suite 200, Frankfort, KY 40601, by calling the Identity Theft Hotline at (877) 438-4338, or visiting their website at https://www.ag.ky.gov/Resources/Consumer-Resources/Consumers/Pages/Identity-Theft.aspx.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx. Navigate360 is located at 3900 Kinross Lakes Parkway, Suite 200, Richfield, Ohio 44286 and can be reached at 330-661-0106.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.

South Carolina residents are advised that they can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for South Carolina's Identity Theft Unit by calling 803-734-4200 or 800-922-1594 (toll-free with SC area code), by email at IDTheftHelp@scconsumer.gov, or visiting the website https://consumer.sc.gov/.