Jeffrey J. Boogay
Office: (267) 930-4784
Fax: (267) 930-4771
Email: jboogay@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 18, 2025

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, IA 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Navia Benefit Solutions, Inc. ("Navia") located at 707 South Grady Way, Suite 350 Renton, WA 98057, and are writing to notify your office of an incident that may affect the security of certain personal information relating to two thousand seven hundred eighteen (2,718) Iowa residents. By providing this notice, Navia does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

On January 23, 2026, Navia discovered suspicious activity related to its environment. Navia promptly responded and launched an investigation to confirm the nature and scope of the incident. The investigation determined that an unauthorized actor accessed and potentially acquired certain information between December 22, 2025, and January 15, 2026. Navia conducted a thorough review of the activity to determine which individuals may have been impacted by this event.

The information that could have been impacted includes name, date of birth, Social Security number, phone number, email address.

Notice to Iowa Residents

On March 13, 2026, Navia began providing notice via substitute notification to potentially impacted individuals. On or about March 18, 2026, Navia began providing written notice of this incident to two thousand seven hundred eighteen (2,718) Iowa residents because information protected by your state law was impacted. Additional individuals residing in Iowa were also notified pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). The 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, Navia moved quickly to investigate and respond to the incident, assess the security of Navia systems, and identify potentially affected individuals. Further, Navia notified federal law enforcement regarding the event. Navia is also working to implement additional safeguards and training for its employees. Navia 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.

Additionally, Navia is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Navia 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.

Navia is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. Navia is also notifying the U.S. Department of Health and Human Services and prominent media pursuant to HIPAA.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,

Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB/sep
Enclosure

EXHIBIT A

<<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 (NOTICE OF SECURITY INCIDENT/ NOTICE OF DATA BREACH)>>

Dear <<first_name>> <<last_name>>,

Navia Benefit Solutions, Inc. ("Navia") writes to make you aware of an event that may affect the security of some of your information. While we are unaware of any attempted or actual misuse of your information at this time, we are providing you with this notice in an abundance of caution, to inform you of the incident, our response, and steps you may take to help protect your information, should you feel it is necessary to do so.

What Happened? On January 23, 2026, Navia discovered suspicious activity related to our environment. Navia promptly responded and launched an investigation to confirm the nature and scope of the incident. The investigation determined that an unauthorized actor accessed and acquired certain information between December 22, 2025, and January 15, 2026. We conducted a thorough review of the activity to determine which individuals may have been impacted by this event. We are notifying you because that investigation determined certain information related to you was impacted.

What Information Was Involved? The review determined your name and the following data elements were impacted: <<b2b_text_2 (data elements)>>. Where potentially impacted, health plan refers only to participation in Health Reimbursement Arrangements (HRAs) and Flexible Spending Accounts (FSAs), or Consolidated Omnibus Budget Reconciliation Act (COBRA). Additionally, potentially impacted data points are limited to items such as termination date and election date. No claims or financial data were disclosed.

What We Are Doing. The confidentiality, privacy, and security of personal information is among Navia's highest priorities, and we have security measures in place to protect information in our care. Upon discovery, we promptly commenced an investigation to confirm the nature and scope of this incident. This investigation and response included reviewing the security of our systems, reviewing the contents of relevant data for sensitive information, and notifying potentially impacted individuals. While we have measures in place to protect information in our care, as part of our ongoing commitment to the privacy of information, we continue to review our policies, procedures and processes related to the storage and access of personal information to reduce the likelihood of a similar future event. Federal law enforcement was notified, and we will also notify applicable regulatory authorities as necessary.

As an added precaution, we are also offering <<ServiceTerminMonths>> months of complimentary access to identity monitoring services through Kroll. Individuals who wish to receive these services must enroll by following the below enrollment instructions, as we are unable to enroll you in the services on your behalf. Please note the deadline to enroll is <<b2b_text_6 (activation deadline)>>.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and credit reports for suspicious activity and to detect errors. You can review the enclosed *Steps You Can Take To Help Protect Personal Information* to learn helpful tips on steps you can take to protect against possible information misuse, should you feel it appropriate to do so.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call Kroll, our external dedicated assistance line at (844) 443-1645, Monday through Friday from 9:00 a.m. - 6:30 p.m. Eastern Time, excluding some U.S. holidays. Or you can also write to Navia directly at 707 South Grady Way, Suite 350 Renton, WA 98057.

Sincerely,

Navia Benefit Solutions, Inc.

Steps You Can Take To Help Protect Personal Information

Enroll in Monitoring Services

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.

How to Activate Your Identity Monitoring Services

1. You must activate your identity monitoring services by **<<b2b_text_6 (Activation Deadline)>>**. Your Activation Code will not work after this date.
2. Visit **Enroll.krollmonitoring.com/redeem** to activate your identity monitoring services.
3. Provide Your Activation Code: **<<b2b_text_ 5 (Activation Code)>>** and Your Verification ID: **<<b2b_text_4 (Verification ID)>>**

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 1-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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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 the relevant 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 event. <<b2b_text_3 (There are approximately [NUMBER] Rhode Island residents that may be impacted by this event.)>>

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit services, you must be 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.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.