HUNTON

HUNTON ANDREWS KURTH LLP
200 PARK AVENUE
NEW YORK, NEW YORK 10166-0005

TEL 212 • 309 • 1000
FAX 212 • 309 • 1100

BRITTANY BACON
DIRECT DIAL: 212 • 309 • 1361
EMAIL: bbacon@hunton.com

November 11, 2026

Via Email (consumer@ag.iowa.gov)

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319

To Whom It May Concern:

In accordance with Iowa Code §§ 715C.1, 715C.2, I am writing on behalf of Vanguard ("Vanguard" or the "Company") to notify you about the nature and circumstances of a data incident.

Vanguard experienced a social engineering incident similar to those recently targeting organizations across the financial services, healthcare, and consumer goods industries. Upon becoming aware of the issue, Vanguard activated its incident response protocols, worked to contain the unauthorized activity, and engaged leading third-party cybersecurity experts. Based on the investigation, Vanguard determined that an unauthorized third party gained access to certain files within a limited number of cloud-based applications between July 29 and 31, 2026.

The incident did not disrupt Vanguard's business operations or services. The investigation found that no client accounts were accessed and there was no unauthorized access to Vanguard's recordkeeping system or any systems that provide the ability to move money. The activity was contained, and there is no evidence of ongoing unauthorized activity associated with the incident.

Based on an extensive review by a third-party data mining vendor, Vanguard determined, on or around October 16, 2026, that the affected files contained personal information associated with certain Vanguard clients. The types of personal information affected vary by individual and may include name, Social Security number, and/or date of birth, and in some cases additional details associated with an individual's account or profile. Not all of these data elements were involved for each affected individual.

Vanguard is providing written notification to approximately 624 Iowa residents who were affected by this issue. The notification offers affected individuals the ability to enroll in three

years of triple-bureau credit monitoring, fraud consultation, and identity theft restoration services through a third-party vendor at no cost to the individual. Vanguard has also arranged to provide a toll-free dedicated call center to support questions from affected individuals and help them enroll in these services. Enclosed for your reference is a sample of the notification being sent to affected individuals.

Please do not hesitate to contact me if you have any questions.

Sincerely,

Brittany Bacon

Enclosure

Vanguard

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

P.O. Box 2600
Valley Forge, PA 19482-2600
vanguard.com

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



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

Re: Notice of Data Breach

Dear <<First_name>> <<Last_name>>,

We are writing to inform you about a data incident that involved some of your personal information associated with your Vanguard account. Importantly, your Vanguard account was not accessed, and the incident did not disrupt Vanguard's business operations or services.

Vanguard is committed to protecting your personal information, which is why we are writing to you with information about the incident, measures we have taken to address this matter, and steps you can take to further protect your information.

What Happened?

Vanguard experienced a social engineering incident between July 29-31, 2026. Social engineering campaigns work when an imposter targets an employee, posing as a legitimate contact, and deceives the employee into providing access to their corporate accounts.

In this case, the incident resulted in a third party gaining unauthorized access to certain files within a limited set of cloud-based applications, like Microsoft 365. Some of those files contained personal information associated with certain Vanguard clients. No client accounts were accessed. There is no evidence of access to Vanguard's recordkeeping system or any system that provides the ability to move money.

Upon becoming aware of the activity, we quickly activated our incident response protocols, took steps to contain the unauthorized activity, and engaged leading third-party cybersecurity experts. The activity was contained and, based on our investigation, there is no evidence of ongoing unauthorized activity. There is also no evidence of any malicious software or ransomware on Vanguard systems associated with the incident.

What Information Was Involved?

We have worked diligently with the assistance of a third-party vendor to determine the nature and scope of the affected data. Based on our investigation, we determined on or around <<b2b_text_2 (discovery date)>>, that certain elements of your personal information were affected by this incident.

The affected personal information varied by affected individual and included your <<b2b_text_1 (data elements)>>, and may have also included additional details associated with your plan.

We do not have any indication that your personal information was specifically targeted.

What We Are Doing

Protecting our client data is a top priority for Vanguard. Beyond the immediate containment steps, Vanguard has taken steps to further strengthen our robust cybersecurity, monitoring controls, and employee training. Vanguard has also been coordinating with law enforcement authorities.

What You Can Do

We recommend that you take the following steps to help further protect your information:

- **Visit our Security Center** for information on how to add features such as security codes and account activity alerts, as well as additional tips and resources to help protect your Vanguard account(s) at https://investor.vanguard.com/security-center.
- **Register for Identity Monitoring Services.** We have arranged to offer you three years of complimentary Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration services through a third party. Please see the pages that follow this letter for information on how to enroll.
- **Order your free credit report.** You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228.
- **Remain vigilant.** We encourage you to review your Vanguard account statements and free credit reports for any unauthorized activity. In addition, it is always a good practice to be cautious of any unsolicited communications that ask for your personal information or refer you to a web page asking for personal information, and avoid clicking on links or downloading attachments from suspicious emails.

For additional information on steps you can take to protect yourself, please see the pages that follow this letter.

For More Information

We have established a dedicated call center at (844) 301-0144, Monday through Friday from 9:00 a.m. to 9:00 p.m., Eastern Time, excluding major U.S. holidays, for further information and answers to any questions you may have.

Protecting our clients' information is a top priority, and we take this matter very seriously. We regret any inconvenience or concern this may cause and are committed to supporting you through this process.

Sincerely,

Vanguard

ADDITIONAL STEPS YOU CAN TAKE

Register for Identity Monitoring Services: To help protect your identity, we have arranged to provide identity monitoring services at no cost to you for three years through Kroll. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have experienced unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration, as detailed below.

How to Activate Your Identity Monitoring Services

You must activate your identity monitoring services by **<<b2b_text_6 (activation deadline)>>**. Your Activation Code will not work after this date.

Visit **Enroll.krollmonitoring.com/redeem** to activate your identity monitoring services.

Provide Your Activation Code: **<<b2b_text_5 (Activation Code)>>** and Your Verification ID: **<<b2b_text_4 (Verification ID)>>**

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

Take Advantage of Your Identity Monitoring Services

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

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—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.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.

Remain Vigilant and Order Your Free Credit Report: We remind you that it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Place a Fraud Alert on Your Credit File: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies.

Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 105069, Atlanta, GA 30348-5069, www.equifax.com, 1-800-525-6285
- *Experian*, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud - an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Report Incidents: 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 state. You can also obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Centre, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Place a Security Freeze on Your Credit File: You have the right to put a security freeze, also known as a credit freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a personal identification number ("PIN") that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. *Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company.* For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, 1-888-909-8872, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348-5788, 1-888-378-4329, www.equifax.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior 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.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique PIN, password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

If you are a resident of Connecticut, Iowa, Maryland, Massachusetts, New York, North Carolina, Oregon, Rhode Island, or Washington D.C., you may contact your state attorney general, including to report suspected identity theft, and obtain information from them about how to protect yourself from identity theft at:

- *Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag
- *Office of the Attorney General of Iowa,* Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, 1-800-373-5044 (toll-free in Iowa) / 515-281-5044, www.iowaattorneygeneral.gov
- *Maryland Office of the Attorney General, Consumer Protection Division*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 (tollfree in Maryland) / 1-410-576-6300, www.oag.state.md.us
- *Office of the Massachusetts Attorney General*, *Consumer Protection Division*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html
- *Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755 (toll-free), 1-800-788-9898 (TDD/TTY toll-free line), www.ag.ny.gov; *Bureau of Internet and Technology (BIT)*, 28 Liberty Street, New York, NY 10005, 212-416-8433, www.ag.ny.gov/resources/individuals/consumer-issues/technology
- *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-877-566-7226 (toll-free in North Carolina) / 1-919-716-6400, www.ncdoj.gov
- *Oregon Department of Justice*, 1162 Court Street NE, Salem, OR 97301-4096, 1-877-877-9392 (toll-free in Oregon), 503-378-4400, www.doj.state.or.us
- *Rhode Island Office of the Attorney General, Consumer Protection Unit*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov
- *Office of the Attorney General for the District of Columbia,* 400 6th Street NW, Washington, D.C. 20001, 202-727-3400, www.oag.dc.gov

If you are a resident of Massachusetts or Rhode Island, note that pursuant to Massachusetts or Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze. As described above, the consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account. <<b2b_text_3 (This incident involves [NUMBER] Rhode Island residents.)>>

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described above.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act ("FCRA"), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you (e.g., denying your application for credit, insurance, or employment) and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days, if you are on welfare, or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active-duty military personnel have additional rights.