Troutman Pepper Hamilton Sanders LLP
5 Park Plaza, Suite 1400
Irvine, CA 92614-2545

troutman.com

Sadia Mirza
sadia.mirza@troutman.com

April 17, 2023
ELECTRONIC MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

To Whom It May Concern:

I am writing on behalf of my client, Virginia Partners Bank, at 410 William Street, Fredericksburg, Virginia, 22401, about a recent data security incident. This incident potentially impacted 3,043 individuals in total, 1,298 of whom are Maryland residents.

Notice of the incident will be sent to the resident via US mail on or about April 17, 2023. A sample copy of the notice being sent to the resident is attached for reference.

Incident and Potentially Impacted Information

On January 12, 2023, a Virginia Partners Bank employee received a suspicious email from a co-worker. The co-worker indicated that he did not send the email. Virginia Partners Bank therefore immediately took steps to secure its email environment and engaged a leading computer forensic firm and cybersecurity experts to investigate to determine what happened. The investigation revealed that on March 27, 2023, certain personal information was accessed or acquired by an unknown third party. Virginia Partners Bank determined that the information may have included your: first and last name, address, Social Security number, health insurance information, or driver's license number

Remedial Steps

Once Virginia Partners Bank became aware of the incident, Virginia Partners Bank immediately commenced an investigation to determine the nature and scope of the issue.. In addition, Virginia Partners Bank is providing impacted individuals with complimentary identity theft protection services for one year, and instructions to individuals on ways to protect their personal information. A description of the benefits and enrollment instructions for the complimentary credit monitoring services will be included in the notice to the impacted resident.

Should you have any questions or concerns about this matter, please do not hesitate to contact me using the contact information provided below.

Sincerely,

Sadia Mirza
Direct: 949.622.2786
sadia.mirza@troutman.com

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

April 17, 2023

Notice of Data <<Security Incident>> <<Breach>>:

Dear <<First Name>> <<Last Name>>:

We write to inform you of a recent data security incident Virginia Partners Bank experienced that may have involved some of your information. Please read this letter as it provides information about the incident and informs you about steps that you can take to help protect your personal information.

What Happened: On January 12, 2023, a Virginia Partners Bank employee received a suspicious email from a co-worker. The co-worker indicated that he did not send the email. Virginia Partners Bank therefore immediately took steps to secure its email environment and engaged a leading computer forensic firm and cybersecurity experts to investigate to determine what happened. The investigation revealed that on March 27, 2023, certain personal information was accessed or acquired by an unknown third party.

What Information Was Involved: Virginia Partners Bank completed a comprehensive review of the data that could have potentially been accessed or acquired by the unauthorized party. On March 27, 2023, Virginia Partners Bank determined that the information may have included your: first and last name, address, Social Security number, health insurance information, or driver's license number. **We have no indication that your information has been misused.**

What We Are Doing: To reduce the likelihood of a similar incident occurring in the future, Virginia Partners Bank has implemented additional measures to enhance the security of its email environment. And we are providing you with information about steps that you can take to help protect your personal information, including offering you complimentary identity protection services through Experian, which includes <<12 months/24 months>> of credit monitoring.

What You Can Do: While we do not have any indication that you information has been misused; we advise you to remain vigilant for signs of unauthorized activity by reviewing your financial statements. We also encourage you to enroll in the complimentary identity protection services through TransUnion. Finally, for more information on how you can protect your personal information, please review the resources provided on the following pages.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the services offered, please call 1-844-787-4607, Monday through Friday between 8:00 a.m. to 5:00 p.m. Eastern Time.

The security of your information is a top priority for Virginia Partners Bank. We take your trust in us and this matter very seriously and we deepl regret any worry or inconvenience that this may cause you.

The consumer reporting agencies have up to three business days after receiving your request 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 personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN or password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze to allow a specific entity or individual access to your credit report, you must make a request to each of the consumer reporting agencies (using the contact information above). You must provide proper identification (including name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period rather than for a specific entity or individual, using the same contact information above. The credit bureaus have up to three business days after receiving your request to lift the security freeze for those identified entities or for the specified period.

To remove the security freeze, you must make a request to each of the consumer reporting agencies using the contact information above. You must provide proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have up to three business days after receiving your request to remove the security freeze. No fee is required to be paid to any of the consumer reporting agencies to place, lift or remove a security freeze.

To determine whether any unauthorized credit was obtained with your information, you may obtain a copy of your credit report at www.annualcreditreport.com or 1-877-322-8228. You may also request information on how to place a fraud alert by contacting any of the above consumer reporting agencies. A fraud alert is intended to alert you if someone attempts to obtain credit in your name without your consent. It is recommended that you remain vigilant for any incidents of fraud or identity theft by reviewing credit card account statements and your credit report for unauthorized activity. You may also contact the Federal Trade Commission (FTC) to learn more about how to prevent identity theft:

FTC, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Please accept my sincere apologies and know that Virginia Partners Bank takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you. If you have questions or need assistance, please call IDX at 1-800-939-4170 from 8:00 A.M. to 8:00 P.M. Central Time, Monday through Friday (excluding holidays). IDX call center representatives are fully versed on this incident and can answer any questions that you may have.

Sincerely,

Virginia Partners Bank

Additional Steps You Can Take to Further Protect Your Information

Order And Review Your Free Credit Report. You can remain vigilant by monitoring your free credit report, which you can order at www.annualcreditreport.com, by calling toll-free at 1-877-322-8228, or by completing the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at https://consumer.ftc.gov/articles/ free-credit-reports and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number, or request form. When you receive your credit report, review it carefully. Look for accounts you did not open, or inaccuracies in your information. If you see anything inaccurate or that you do not understand, contact the consumer reporting agency.

Report Identity Theft or Fraud to FTC, Law Enforcement, and Attorneys General. You can remain vigilant by reviewing financial account statements for fraudulent transactions or identity theft. If you detect any unauthorized transactions in a financial account, promptly notify your financial institution. If you detect any incident of identity theft, promptly report the incident to law enforcement, the FTC, and your state Attorney General.

Learn More About Identity Theft From the FTC. You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft: Federal Trade Commission Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft/ and www.identitytheft.gov.

Fraud Alerts on Your Credit File. To help protect yourself from possible identity theft, consider placing a fraud alert on your credit file. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. For more information on fraud alerts, you can contact the consumer reporting agencies listed below or the FTC.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-685-1111	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion Consumer Solutions P.O. Box 2000 Chester, PA 19016	1-800-909-8872	www.transunion.com

Security Freezes on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. A security freeze must be placed on your credit file at each consumer reporting agency individually. For more information on security freezes, you can contact the consumer reporting agencies listed above or the FTC. As the instructions and fees (if any) for placing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information. The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide: your full legal name, Social Security Number, date of birth, addresses where you have lived in the past five years, copies of government-issued identification cards, and proof of your current address.

Additional Rights Under the FCRA. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act by: (i) visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf; or (ii) by writing to Consumer Financial Protection Bureau, 1700 G Street, N.W., Washington, DC 20552.

For Maryland Residents. You can obtain information about avoiding identity theft from the Maryland Attorney General at: Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place Baltimore, MD 21202, (888) 743-0023 (toll-free in Maryland), (410) 576-6300, www.marylandattorneygeneral.gov.

For New York Residents. You can obtain information about security breach response, identity theft prevention, and identity protection information from the New York State Office of the Attorney General at: 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), https://ag.ny.gov/, and at: Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005, Phone: (212) 416-8433, https://ag.ny.gov/internet/resource-center.

For North Carolina Residents. You can obtain information about avoiding identity theft from the North Carolina Attorney General at: North Carolina Attorney General's Office 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free in North Carolina), (919) 716-6400, www.ncdoj.gov.

For Residents of Oregon. You may report suspected identity theft to law enforcement, including the Office of the Oregon Attorney General and the FTC. Contact information for the FTC is included in your notice. The Office of the Oregon Attorney General can be reached: (1) by mail at 1162 Court St. NE, Salem, OR 97301; (2) by phone at (877) 877-9392; or (3) online at https://www.doj.state.or.us/.

For Rhode Island Residents. You can obtain information about avoiding identity theft from the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, Consumer Protection Unit 150, South Main Street, Providence, RI 02903, (401)-274-4400, www.riag.ri.gov. Data on approximately Rhode Island residents were involved in this incident. You have the right to obtain a police report, and to request a security freeze (charges may apply), as described above.

For Washington, D.C. Residents. You can obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia at: 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. You have the right to request a security freeze (without any charge) as described above.

TransUnion

Enter your Activation Code: ***<<ACTIVATION CODE>>***
Enrollment Deadline: ***<<Enrollment Deadline>>***

1-Bureau TransUnion Credit Monitoring Product Offering: (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for <<Insert 12 months or 24 months>> provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code ,**<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your creditmonitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<< Insertstatic 6-digit Telephone Pass Code >>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain << Insert 12 months or 24 months >> of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit reportonline, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and <<Insert Date>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.