EXHIBIT A

1_0000080

DE 1931
Commonwealth
TRUST COMPANY

September 19, 2025

Dear

We are writing to inform you of a recent incident that may impact the security of some of your personal information. While we are unaware of any attempted or actual fraudulent use of your information, we are providing you with details about the incident, our response, and steps you may take to protect against potential misuse of your information, should you wish to do so.

What Happened? Earlier this year, we learned of suspicious activity related to a Commonwealth Trust Company ("CTC") employee email account. In response, we launched an investigation to determine what occurred and confirm the security of our email environment. During our review, we identified that an unauthorized actor accessed a CTC e-mail account for a limited period of time on May 13, 2025, and obtained emails from the account. We then performed a thorough review of the contents of the impacted email account to determine if it contained sensitive information and, if so, to whom the information related. We completed our review on August 4, 2025. We have worked since this time to verify the information at issue and confirm current address information in order to provide this notice to you.

What Information Was Involved? The following types of information were contained in the email account at the time of the incident: name, treating/referring physician, patient account number, account number, treatment information, prescription/medication information, individual insurance/subscriber number, account number with bank name, Social Security number, medical record number, medical billing/claims information, other health insurance information, and date of birth.

What We Are Doing. We take this incident and the security of information in our care very seriously. Upon learning of this incident, we immediately secured the account and undertook a comprehensive investigation. As part of our response, we implemented supplemental technical and administrative security measures. We are notifying potentially impacted parties to make them aware of this incident and are providing them with access to **Single Bureau Credit Monitoring, Single Bureau Credit Report, and Single Bureau Credit Score** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Enrollment instructions are enclosed with this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your relevant account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. If fraudulent activity is identified, promptly report it to the relevant organization and law enforcement. We also recommend you review the enclosed *Steps You Can Take To Help Protect Personal Information* for useful information on what you can do to better protect against possible misuse of your information. You may also enroll in the complimentary credit monitoring services we are offering you. Please note that, due to privacy restrictions, we are unable to automatically enroll you in the complimentary credit monitoring services.

For More Information. If you have further questions or concerns, please contact Jamie McGinley, Managing Director, and Rebecca Shimkus, Chief Financial Officer, at 302-358-7214, or write to us at 29 Bancroft Mills Road, Wilmington, DE 19806. If you have any questions about the credit monitoring services being offered or to enroll in these services, please call 1-800-405-6108 from Monday through Friday, between 8:00 am to 8:00 pm Eastern Time (excluding holidays). We continue to devote significant resources to protect and maintain the confidentiality of information entrusted to us and regret any inconvenience or concern this incident may cause you.

Sincerely,

Rebecca Shimkus
CHIEF FINANCIAL OFFICER

0000080

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: 2A7C7A5B5A04 In order for you to receive the monitoring services described above, you must enroll within 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.

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 their 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 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.