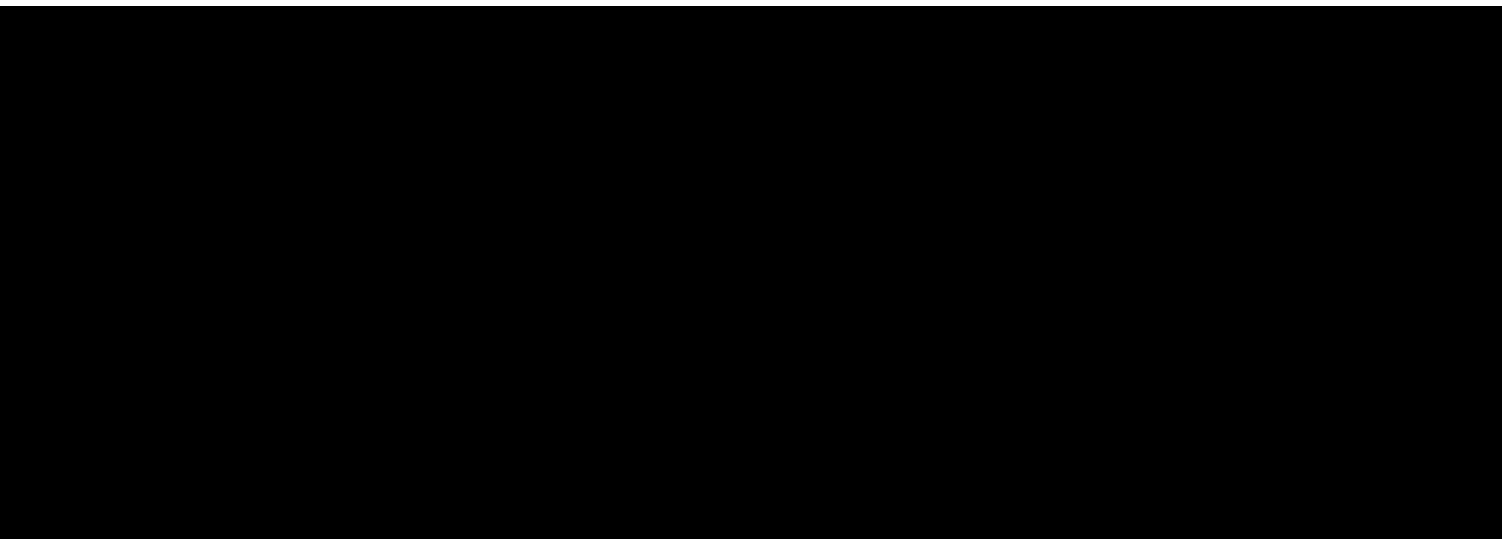


Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Via email to ldtheft@aog.state.md.us

Dear Attorney General Frosh,

This email is to report a security breach affecting 13 Maryland residents, as required by the Personal Information Protection Act. A copy of the 4-page notice that will soon be sent to residents is attached.

Brief description:

On December 27, 2021, a third-party contractor ("Contractor") notified Truist of a December 23 disruption to Contractor's computer systems used to process Truist sensitive personal information ("PI"). The disruption was later attributed to a malware cyberattack ("cyberattack"). Truist and Contractor coordinated closely through January 2022 to understand the scope of the attack, any exposure of PI to unauthorized individuals, and any risk of harm from such exposure. On March 25, 2022, Contractor notified Truist that further investigation revealed that Truist PI had been exfiltrated by the attacker. 13 Maryland residents' Social Security numbers were found among 32 separate files containing 16,000 pages of non-structured data. It is therefore unlikely that the PI would be sought, found, and used for identity theft or other malicious purposes.

Restoring system/information integrity:

The Contractor reported to Truist that Contractor systems were returned to service using clean sources, including uncorrupted data sets. Truist has since increased security requirements on Contractor through updated contracts.

Respectfully submitted on behalf of Truist Financial Corporation,

David Delaney (he/him/his)
Vice President
Assistant General Counsel, Cybersecurity & Privacy
CIPP/US
Office: 919-424-0883
david.delaney@truish.com
LinkedIn: [David Delaney](#)



The information transmitted is intended solely for the individual or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of or taking action in reliance upon this information by persons or entities other than the intended recipient is prohibited. If you have received this email in error please contact the sender and delete the material from any computer.



Truist HR Teammate Relations
214 N. Tryon Street - 500-93-45-10
Charlotte NC 28202

April 14, 2022



Re: Notice of Information Security Incident

Dear :

We are writing to inform you about an information security incident involving your sensitive information. We take the privacy of your information very seriously and are sending you this letter to inform you about what occurred, provide you with complimentary credit and identity monitoring services, and inform you about additional steps you can take to protect your sensitive information.

What Happened?

A third-party contractor recently notified Truist that personal information used to generate teammate benefit information letters in 2008 was potentially exposed to unauthorized individuals beginning in December 2021. Truist worked closely with the contractor to understand the scope of the incident and the information that was exposed. Services to Truist have been restored using systems and personal information that were not affected during the incident. In addition, Truist is increasing security requirements for such contractors to better protect your information.

What Information Was Involved?

The personal information that may have been exposed included name, address, Social Security Number, and date of birth.

What We Are Doing.

Although we do not suspect any misuse of your information, we want to offer you an identity theft credit monitoring subscription service to help prevent and detect any misuse of your information. This is a complimentary two-year membership to Experian CSIdentity. This product helps detect possible misuse of your personal information, and provides you with identity protection support focused on immediate identification and resolution of identity theft. Below are instructions to enroll.

Three Easy Steps to Enroll:

1. Enroll by July 31, 2022
Activate membership by visiting CSIdentity Web Site:
<https://portal.idnotify.com/enrollment/34?RTN=90000122>
2. Activation code: 753FI354YL
3. If you have questions or need an alternative to enrolling online, please call Experian CSIdentity Corporation at 888-852-7176

What You Can Do.

We recommend that you follow the instructions for identity theft enrollment, and to protect your personal information. We also recommend that you review your financial activity and account statements.

For More Information

More information about steps you can take to further protect your personal information are included.

The security of your personal information has been, and remains our highest priority. Should you have any questions, please contact Truist Customer Care at 844-487-8478. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Truist Customer Care

Enclosure



STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Accounts and Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.com

Free Annual Report

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 12 months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You are encouraged to report suspected identity theft to the FTC.

**Federal Trade
Commission**

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

If you are a resident of North Carolina or Maryland, you may also report suspected identity theft to local law enforcement, including the Attorney General in your state.

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

Residents of other states can find contact information for each Attorney General at www.naaq.org/naaq/attorneys-general/whos-my-ag.php.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>