



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

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

LISA SOTTO  
DIRECT DIAL: 212 • 309 • 1223  
EMAIL: lsotto@Hunton.com

FILE NO: 033411.0000099

August 14, 2024

**Via Email** (idtheft@oag.state.md.us)

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

To Whom It May Concern:

In accordance with Md. Code Ann. Com. Law § 14-3504, I am writing on behalf of Truist Financial Corporation (“Truist”) to notify you regarding the nature and circumstances of a data security issue.

On or around October 27, 2023, an unauthorized third party gained access to a small number of Truist employee user accounts. The unauthorized party used these user accounts to obtain the information of some Truist clients. At that time, Truist’s cybersecurity team promptly took steps to assess the intrusion and contain the unauthorized access. Recent findings from Truist’s continued collaboration with law enforcement and outside cybersecurity experts has led to new information about the issue. On June 27, 2024, Truist was able to determine that a portion of the affected files contained some personal information of Maryland residents, such as name and Social Security number.

Truist is notifying approximately 92 Maryland residents whose personal information was identified in the relevant files. Truist has arranged to offer 24 months of identity monitoring services at no cost to these affected individuals. Enclosed for your reference is a sample of the notice being sent to affected individuals.

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

Very truly yours,

Lisa J. Sotto

Enclosure

[Insert date], 2024

[Name]

[Address]

[City], [State] [ZIP]

Dear [Name],

Thank you for being a valued Truist client. We strive to serve all our clients with transparency and care.

We are reaching out to notify you about a security incident that resulted in unauthorized access to and acquisition of some of your personal information. We have found no fraud linked to this incident. That said, Truist will continue to monitor the situation with our goal being to minimize possible impact to you.

We sincerely apologize for any inconvenience this may cause. We are here to support you and to provide useful resources, including credit monitoring and identity protection services at no cost to you. Below are more details about this incident, the actions we took to address it, and the steps we recommend for you to protect your information.

### **What Happened?**

Around October 27, 2023, an unauthorized third party gained access to a small number of Truist employee accounts. This unauthorized party used these accounts to obtain the information of some Truist clients. At that time, our cybersecurity team promptly took steps to assess the intrusion and contain the unauthorized access. Recent collaboration with law enforcement and outside cybersecurity experts has led to new information about the incident. On July 2, 2024, Truist was able to determine that a portion of the affected files contained some of your personal information.

### **What Information Was Involved?**

The affected files contain a limited amount of your personal information, such as name and Social Security number.

### **What We Are Doing**

Truist works hard to monitor our networks and platforms, protect sensitive information, and implement cybersecurity safeguards. We have found no indication of fraud arising from this incident and continue to monitor your accounts to mitigate potential fraud risk. We are also working closely with law enforcement to support their criminal investigation.

## What You Can Do

Our clients' privacy and security is a top priority at Truist. Our relationship with our clients is built on a foundation of trust, which we value greatly and work very hard to protect. At this time, we are not aware of any fraudulent activity on your Truist accounts related to this incident. However, we want to share some actions you can take to help protect your information:

- **Register for Identity Protection Services:** We will provide you credit monitoring and identity protection services for 24 months at no cost to you. The enclosed Reference Guide provides instructions on how to enroll in these services.
- **Request a New Account Number:** Work with your local relationship manager to have new account number(s) issued.
- **Order a Credit Report:** You are entitled to one free credit report annually from each of the three national consumer reporting agencies. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call (877) 322-8228.
- **Monitor Your Accounts:** We encourage you to monitor your accounts closely over the next 12-24 months. Review your account statements and your free credit reports closely. If you notice any suspicious activity, report your concerns to your local Truist relationship manager immediately.
- **Review the Enclosed Reference Guide:** The enclosed Reference Guide has further guidance for protecting your personal information.

## For More Information

Please know how much we value your relationship with Truist. If you have any questions regarding this issue, please call Truist Client Care at (844) 487-8478, Monday-Friday from 8am-8pm (EST) and Saturday from 8am-5pm (EST).

Sincerely,

Truist Client Care

## Reference Guide

We encourage affected individuals to take the following steps:

### **Register for Identity Protection Services.**

We have arranged for you to receive a complimentary subscription of Experian's CSIdentity. The CSIdentity service includes daily monitoring of your credit reports from the three nationwide credit reporting agencies (Experian®, Equifax® and TransUnion®), identity theft monitoring and restoration and email monitoring alerts of key changes to your credit reports. This service will expire at the conclusion of the complimentary two-year period and will not automatically renew. Truist is not involved with respect to any offers, products, or services from or through CSIdentity Corporation, a part of Experian, that you choose to enroll in beyond the complimentary subscription.

Enter the activation code below at CSIdentity website link for enrollment in your complimentary subscription. You may also enroll via phone.

- CSIdentity Corporation Web Site: <https://portal.idnotify.com/enrollment/34?RTN=90000122>
- Enrollment by phone or if you need help, call Experian CSIdentity Corporation at (888)883-1852.
- Activation Code: [Unique pin code for each individual]
- You must enroll by: [DATE]

**Order Your Free Credit Report.** To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov) and mail 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. Look in the "inquiries" section for names of creditors from whom you have not 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.

### **Further Steps You Can Take to Protect Your Information**

- Don't open emails, click links or download attachments from questionable sources.
- Don't believe in tempting offers. If you think a deal is too good to be true, it probably is.
- Use strong, unique passwords for your online accounts.
- Make sure you are using an updated antivirus software.
- Don't answer to any requests for passwords.

**Report Incidents.** We encourage you to review your account statements and immediately report any suspicious activity to us. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

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/](http://www.ftc.gov/idtheft/)

**Consider Placing 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. For more information on fraud alerts, you also may contact the FTC as described above.

|            |                                                                          |                |                    |
|------------|--------------------------------------------------------------------------|----------------|--------------------|
| Equifax    | Equifax Information Services LLC<br>P.O. Box 740241<br>Atlanta, GA 30374 | (800) 525-6285 | www.equifax.com    |
| Experian   | Experian Inc.<br>P.O. Box 9554<br>Allen, TX 75013                        | (888) 397-3742 | www.experian.com   |
| TransUnion | TransUnion LLC<br>P.O. Box 2000<br>Chester, PA 19016                     | (800) 680-7289 | www.transunion.com |

**Consider Placing a Security Freeze on Your Credit File.** You may wish to place a “security freeze” (also known as a “credit 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. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing 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 name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)