TRUST COMPANY OF THE SOUTH

April 24, 2018

"Identifier" "First Name" "Last Name"
"Address1"
"Address2"
"Address3"
"City", "State" "Zip"

NOTICE OF DATA BREACH

Dear "Greeting":

We are writing to advise you of a data security incident that affected our email system. Some of your personal information was included in our email system, so we want to let you know what occurred, what we are doing to address it, and how you can enroll in consumer protection services we are offering. We want to emphasize that our expert's investigation concluded it was unlikely any personal information was taken in this incident, but we value your trust and believe it is important to notify you so that you can take steps to protect yourself. We take privacy and data security very seriously, and we deeply regret that this incident occurred.

What Happened?

On March 19, 2018, we discovered that an unauthorized individual had gained access to our email system. We immediately eliminated the unauthorized access and also implemented additional access controls to prevent further access. We engaged legal counsel who hired a forensic investigator to determine what had occurred and whether any of our clients were affected and if so to what extent.

The investigation concluded on April 19, 2018. The forensic expert determined that the unauthorized access occurred between March 8th and March 19th, and was limited to our email system. It did not impact any other information systems or financial accounts. Our emails did, however, include some of your personal information, such as your "Field1""Field2" The forensic investigation found no evidence that these emails were downloaded or forwarded out of the system. The investigation also concluded that the unauthorized individual appeared to be looking for information to perpetrate wire transfer fraud, although there were no successful wire transfer requests made. We believe this evidence indicates it is unlikely this individual was seeking personal information or sought access for that purpose. However, we believe it is important to notify you in keeping with our compliance obligations and our relationship to you. We also wanted to contact you so we could offer consumer protection services.

What Information Was Involved?

Some personal information was included in the emails in our system, such as your "Field3". However, our forensic expert found no evidence that the emails including personal information were downloaded or forwarded, and we have no indication that any information about you has been misused.

What We Are Doing.

As described above, as soon as we discovered the unauthorized access we eliminated it by terminating and reissuing all access credentials. We promptly engaged legal counsel and a forensic expert, who launched an investigation. We implemented additional access controls and enhanced system logging, and we will continue to evaluate additional controls. We are now notifying you so that you can take steps to protect yourself, such as enrolling to receive the consumer protection services described below.

We have secured the services of CyberScout to provide identity monitoring services at no cost to you for two years. These services include access to ***Single Bureau Credit Monitoring**** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. We are also providing you with $25,000 of identity theft expense reimbursement insurance.

To enroll in **Credit Monitoring*** services at no charge, please log on to **https://www.myidmanager.com** and follow the instructions provided. **When prompted please provide the following unique code to receive services:**
"Code" <code 2>

For guidance with the CyberScout services, or to obtain additional information about these services, **please call the CyberScout help line at *1-800-405-6108,*** available 24 hours a day, 7 days a week (except Thanksgiving Day and Christmas Day), and supply the fraud specialist with your unique code.

What You Can Do.

As noted above, our forensic investigation found no evidence that the emails or email attachments including personal information were downloaded or forwarded, and we have no indication that any information about you has been misused. However, we understand you will be concerned about this incident. The enclosed "Additional Important Information" describes steps you can take to protect yourself, such as remaining vigilant by regularly reviewing your account statements and monitoring credit reports. This enclosure also provides contact details for the Federal Trade Commission and credit reporting agencies and information on how to place fraud alerts and security freezes.

For More Information.

We deeply regret that this incident occurred, and we offer our sincerest apologies. It is not consistent with the trust relationship we have established with you. We want to give you our strongest assurance that we are taking all appropriate steps to mitigate it.

If you have questions, please call **the CyberScout help line at 1-800-405-6108**, available 24 hours a day, 7 days a week (except Thanksgiving Day and Christmas Day). If you would like additional information after calling the help line, please call your relationship manager.

Sincerely,

William H. Smith
President & CEO
Trust Company of the South

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18. 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.

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont, Wyoming,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri, North Carolina*, *Oregon*, and *West Virginia*:

State law requires you to be informed that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 22104	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

You may also obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:

State laws advises you to report any suspected identity theft to law enforcement, as well as to the Federal Trade Commission.

For residents of *Maryland, North Carolina,* and *Illinois*:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General	**North Carolina Office of the Attorney General**	**Federal Trade Commission**
Consumer Protection Division	Consumer Protection Division	Consumer Response Center
200 St. Paul Place	9001 Mail Service Center	600 Pennsylvania Avenue, NW
Baltimore, MD 21202	Raleigh, NC 27699-9001	Washington, DC 20580
1-888-743-0023	1-877-566-7226	1-877-IDTHEFT (438-4338)
www.oag.state.md.us	www.ncdoj.com	www.ftc.gov/bcp/edu/microsites/idtheft

For residents of *Massachusetts*:

State law requires you to be informed of your right to obtain a police report if you are a victim of identity theft. The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three credit bureaus is above.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, or regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a small fee to place, lift, or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. You may obtain a security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp	https://www.experian.com/freeze/center.html	https://freeze.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed above.

For more information regarding steps you can take if you are concerned about fraudulent tax filings, please consult the IRS webpage https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft.