

EXHIBIT A

Trust Company

of Illinois

Dear [REDACTED]:

As a valued client, we write to notify you of a recent data privacy incident involving the Trust Company of Illinois. This notification provides details on the incident, the investigation, and steps we have and are taking in response to the incident.

On April 27, 2018, we learned that a Trust Company of Illinois employee email account was unknowingly used to send phishing emails. Upon learning of the incident, we immediately disabled the account, reset all account passwords and launched an investigation into the nature and scope of the incident. We also worked with third-party forensic investigators to confirm the security of the email account and determine whether sensitive information may have been impacted by the incident. With the assistance of the third-party investigators, we learned that on April 25, 2018, an unauthorized actor gained access to one (1) Trust Company of Illinois email account.

After a thorough and detailed review of the contents of the accessed account, we subsequently determined that information relating to some participating employees, including name, date of birth and/ or Social Security number was potentially accessible. To date we have no evidence to suggest that your employees' information was subject to actual or attempted misuse as a result of this incident. In fact, available forensic evidence suggests that the intent was to defraud our firm in a common wire transfer scheme. Neither Trust Company of Illinois's network nor participant recordkeeping software were affected.

We consider the privacy of your information in our care as a great responsibility. Since discovering this incident, we have been working diligently with third-party forensic investigators to determine what happened and what information was accessible to the unauthorized actor. This has involved a time consuming, programmatic and manual data review process. In an abundance of caution, we are prepared to notify the affected participating account holders by the attached sample notification letter. This includes an offer for complimentary credit monitoring services. We are also providing notice of this event to certain regulators where required. We have also reinforced existing security protocols to recognize popular phishing schemes and reduce the likelihood of a similar email event from occurring in the future. Please contact us directly within five business (5) days if you do not wish Trust Company of Illinois to notify your affected employees on your behalf. If we do not hear from you, we will assume you approve of the letter and notification plan.

As data privacy attacks increase in frequency and sophistication we continue to make the security of personal information in our system a top priority and we apologize for any inconvenience or concern this incident may have caused you. If you have any questions or concerns, please do not hesitate to contact us at [(xxx) xxx-xxxx/xxxxx@xxx.com]

Sincerely,

William M.Giffin

Trust Company of Illinois

EXHIBIT B

Trust Company

of Illinois

Processing Center • P.O. BOX 141578 • Austin, TX 78714



00001
R817801

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

June 29, 2018

Re: Notice of Data Breach

Dear John Sample:

The Trust Company of Illinois recently learned of a data privacy incident that could affect the security of your personal information. To date, we have no evidence to suggest your information was subject to actual or attempted misuse as a result of this incident. However, we take this incident seriously and are providing you with information and access to resources so that you can better protect your personal information should you feel it is appropriate to do so.

What Happened? On April 27, 2018, we learned that a Trust Company of Illinois employee email account was unknowingly used to send phishing emails. Upon learning of the incident, we immediately disabled the account, reset all account passwords and launched an investigation into the nature and scope of the incident. With the assistance of third-party investigators we confirmed that on April 25, 2018, an unauthorized actor gained access to one (1) Trust Company of Illinois email account.

What Information Was Involved? After our investigation and a time-consuming programmatic and manual data review, we determined that your name, date of birth and/or Social Security number were contained in the single email account and were potentially accessible. As noted, to date we have no evidence to suggest your information was subject to actual or attempted misuse as a result of this incident. Except for the one email account, no other part of Trust Company of Illinois' network was affected including your investment accounts.

What We Are Doing? We consider the privacy of your information in our care as a great responsibility. We are providing you notice of this incident and complimentary access to credit monitoring services (discussed further below) in an abundance of caution. We also notified your plan administrator and are notifying certain regulators as required. We have also reinforced existing security protocols to recognize popular phishing schemes and reduce the likelihood of a similar email event from occurring in the future.

What You Can Do. You can enroll and receive the free credit monitoring and identity restoration services we are offering through AllClear ID. You can also review the enclosed *Steps You Can Take to Protect Your Information* for additional details on how to better protect against potential misuse of your information.



01-02-1

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our assistance line at 1-855-309-2010, Monday through Saturday, 8:00 a.m. to 8:00 p.m. CT, excluding major U.S. holidays.

As data privacy attacks increase in frequency and sophistication we continue to make security of personal information on our system a top priority and we apologize for any inconvenience or concern this incident may have caused you.

Sincerely,

William M. Giffin

The Trust Company of Illinois

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-309-2010 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-309-2010 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

Monitor Your Accounts

Credit Reports and Account Statements. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit card and account statements and monitoring your free credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all your credit files. In order to request a security freeze,



you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze/place-credit-freeze

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the credit reporting agencies listed above, Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, 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 violator. 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 visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400.



00002

R817801

JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

June 29, 2018

Re: Notice of Data Breach

Dear John Sample:

Trust Company of Illinois/TC Wealth Partners recently learned of a data privacy incident that could affect the security of your personal information. To date, we have no evidence to suggest your information was subject to actual or attempted misuse as a result of this incident. However, we take this incident seriously and are providing you with information and access to resources so that you can better protect your personal information should you feel it is appropriate to do so.

What Happened? On April 27, 2018, we learned that an employee's email account was unknowingly used to send phishing emails. Upon learning of the incident, we immediately disabled the account, reset all account passwords and launched an investigation into the nature and scope of the incident. With the assistance of third-party forensic investigators we confirmed that on April 25, 2018, an unauthorized actor gained access to one (1) employee email account.

What Information Was Involved? After our investigation and a time-consuming programmatic and manual data review, we determined that your name, date of birth and/or Social Security number were contained in the single email account and were potentially accessible. As noted, to date we have no evidence to suggest your information was subject to actual or attempted misuse as a result of this incident. Except for the one email account, no other part of Trust Company/TC Wealth Partner's network was affected, including your investment accounts.

What We Are Doing? We consider the privacy of your information in our care as a great responsibility. We are providing you notice of this incident and complimentary access to credit monitoring services (discussed further below) in an abundance of caution. We are also notifying certain regulators as required. We have also reinforced existing security protocols to recognize popular phishing schemes and reduce the likelihood of a similar email event from occurring in the future.

What You Can Do. You can enroll and receive the free credit monitoring and identity restoration services we are offering through AllClear ID. You can also review the enclosed *Steps You Can Take to Protect Your Information* for additional details on how to better protect against potential misuse of your information.



01-02-1

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. Should you have additional questions, please contact your relationship manager. To discuss credit services or to enroll in credit monitoring, please call our assistance line at 1-855-309-2010, Monday through Saturday, 8:00 a.m. to 8:00 p.m. CT, excluding major U.S. holidays.

As data privacy attacks increase in frequency and sophistication we continue to make security of personal information on our system a top priority and we apologize for any inconvenience or concern this incident may have caused you.

Sincerely,

William M. Giffin

TC Wealth Partners/Trust Company of Illinois

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-309-2010 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-309-2010 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

Monitor Your Accounts

Credit Reports and Account Statements. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit card and account statements and monitoring your free credit reports for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a “fraud alert” on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer’s credit report without the consumer’s written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all your credit files. In order to request a security freeze,



you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze/place-credit-freeze

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the credit reporting agencies listed above, Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, 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 violator. 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 visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400.