

Morgan Lewis

Gregory T. Parks

Partner
215.963.5170
gregory.parks@morganlewis.com

September 8, 2023

VIA EMAIL TO IDTHEFT@OAG.STATE.MD.US

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

Re: Notice of Data Security Incident of Progress Software as Vendor to Fidelity National Information Services, Inc. and Community Trust Bank, Inc.

Dear Office of the Attorney General:

This Firm represents Fidelity National Information Services, Inc. ("FIS") and we are writing to notify your office on behalf of FIS and its client, Community Trust Bank, Inc. ("CTBI"), regarding the nature and circumstances of a recent data security incident involving the secure file transfer software tool MOVEit Transfer provided by third-party vendor Progress Software.

On May 31, 2023, Progress Software announced a previously unknown critical zero-day vulnerability in MOVEit Transfer and recommended users disable the software until it could be patched due to a potential risk of data exposure. FIS immediately ceased using MOVEit Transfer and disabled it in its system. Later in the evening on May 31 and in the early morning of June 1, 2023, Progress Software released patches to remedy the vulnerability, which FIS successfully deployed the same day on all instances of the MOVEit Transfer applications within its environment. In parallel to the patching activity, FIS immediately launched an investigation with the assistance of cyber experts to assess the scope of the potential exploitation of the vulnerability and notified law enforcement. The investigation revealed that an unauthorized third party may have taken certain of CTBI's files that were transferred from CTBI to FIS through MOVEit Transfer that likely contained personal information of CTBI's customers. Following FIS's investigation, FIS discovered that certain files that contain CTBI's personal information were accessed and potentially removed from the service provider's network by an unauthorized party on May 29-30, 2023, and notified CTBI of this discovery on August 9, 2023.

During the investigation, FIS and CTBI have determined that the impacted files may have included name, date of birth, Social Security number and/or bank account information of CTBI's customers in Maryland. Although there is no indication that the disclosed personal information has been used for any fraudulent purpose, CTBI is sending notifications by mail to the affected individuals to explain what happened, what information was involved, what they and FIS have done, and how

Morgan, Lewis & Bockius LLP

1701 Market Street
Philadelphia, PA 19103-2921
United States

 +1.215.963.5000
 +1.215.963.5001

State of Maryland
Office of the Attorney General
September 8, 2023
Page 2

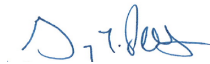
affected individuals can contact CTBI with questions. FIS and CTBI are offering two years of credit monitoring to affected customers of CTBI.

FIS carefully evaluates the cybersecurity posture of third-party file transfer tools, and FIS will continue this effort. FIS is also taking steps to further secure its use of all third-party transfer tools.

Further information about what FIS and CTBI have done and are recommending to the individuals in question can be found in the enclosed notification that CTBI is sending to 37 Maryland residents via mail on September 8, 2023.

If you have any questions, please feel free to contact me.

Regards,

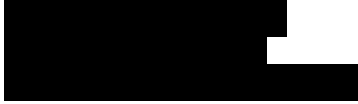
A handwritten signature in blue ink, appearing to read "G. T. Parks", is written over a faint horizontal line.

Gregory T. Parks

Enclosure

Community Trust Bank, Inc.
346 North Mayo Trail
Pikeville, KY 41501

00000001 MMVITBL0907230117641 00000 01 000000 00000001 004



September 8, 2023

RE: NOTICE OF DATA SECURITY EVENT

Dear Valued Customer:

We are writing to provide you with information regarding a recent third-party data incident which involves the security of some of your personal information. As such, we wanted to provide you with information about the incident, explain the services that are being made available to you, and let you know that we continue to take significant measures to protect your information.

What Happened

One of our service providers received notice from one of its third-party vendors, MOVEit, regarding a security vulnerability in the MOVEit Transfer solution which is utilized by our service provider to transmit data. MOVEit reported a zero-day vulnerability in MOVEit Transfer which has been actively exploited by unauthorized actors to gain access to data stored on the MOVEit server. MOVEit has acknowledged the vulnerability and has since provided patches to remediate the exploit. There was no compromise of our service provider's or our broader network security. The Bank's systems were not involved in this incident or compromised in any way.

What We Are Doing

Upon being informed of the vulnerability, our service provider immediately took actions to mitigate and assess the scope of information potentially compromised, including engaging third-party professionals to assist in the investigation and remediation of the vulnerability. Following our service provider's investigation, they discovered on July 24, 2023 that certain files that contain your personal information were accessed and potentially removed from the service provider's network by an unauthorized party on May 29-30, 2023. We were notified of this discovery on August 9, 2023. Our service provider is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident.

What Information Was Involved?

The information potentially accessible on the MOVEit server may have included your

[REDACTED]

What You Can Do

We have no evidence that any of your information has been used to commit financial fraud. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.



To help protect your identity, our service provider is offering a complimentary 24-month membership to OnAlert™ (Essential Bundle) from ChexSystems®. OnAlert provides you with identity monitoring and can assist with the resolution of identity theft. **To activate your membership in OnAlert and start monitoring your personal information please enroll at [REDACTED] by December 31, 2023.** Your link will not work after this date. You will need to provide the website link noted above as proof of eligibility for this offer.

00000001 00001 001-008

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call the dedicated toll-free response line that has been set up to respond to questions at [REDACTED] This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information.

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 24 months Credit Monitoring

For new member questions and assistance with enrollment, please contact the OnAlert customer care team at [REDACTED]. A credit card is not required for enrollment into OnAlert. The response line is available Monday through Friday, [REDACTED] with Saturday and Sunday hours from [REDACTED].

With OnAlert (Essential Bundle), you will have access to the following features:

- **Single-Bureau Credit Report and Manual VantageScore® from Experian®***: Credit reports and scores from Experian.
- **Single-Bureau Credit Monitoring from Experian**: Actively monitors Experian files and alerts you of key changes and indicators of fraud.
- **Automatic VantageScore Tracker**: Shows you your credit score so you can see how lenders evaluate your creditworthiness.
- **VantageScore Simulator**: Interactive credit score simulator you can use to see how actions will potentially impact your Experian credit score.
- **Personalized Credit & Identity Alert Videos**: Credit and identity education videos.
- **Real Time Authorization Alerts**: Notifications of when your personal information is used for new applications or identity authorizations.
- **Dark Web Monitoring**: Internet and dark web surveillance monitoring of your personal information.
- **ChexSystems Monitoring and Alerts**: Actively monitors ChexSystems' database and alerts you of key activity and indicators of fraud. Chex Systems, Inc. (ChexSystems) is a nationwide specialty consumer reporting agency under the Fair Credit Reporting Act (FCRA).
- **Full-Service Restoration**: Certified Identity Theft Restoration Specialists available for assignment to help you address credit and non-credit related fraud.
- **Lost Wallet Assistance**: Protection of your personally identifiable information that has been compromised.
- **Up to \$1M Identity Theft Insurance****: Reimbursement for certain ancillary expenses associated with restoring your identity.

* Calculated on the VantageScore 3.0 model. Your VantageScore 3.0 from Experian® indicates your credit risk level and is not used by all lenders, so don't be surprised if your lender uses a score that's different from your VantageScore 3.0.

**The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 24 month credit monitoring services, we recommend that you place an initial one (1) year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.



Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. **Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. 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 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.



OnAlert™ is here to help you.

Protect yourself from identity theft.

Sign up for a free trial today: <https://onalert.info/communitytrustbank>

How OnAlert™ helps.

As cyber threats continue to increase, OnAlert offers the information, education and protection you need. Plus OnAlert has access to ChexSystems® data that no other provider in the market has today, to help make sure you're safe and secure.



Monitoring



Alerts



Restoration



Education

Identity protection helps to safeguard your good credit and overall financial wellness from growing threats.

OnAlert™ provides an all-in-one solution for all of your financial wellness needs:



Detect fraud quickly:

Monitor your personal information and be alerted if it's detected. OnAlert will alert you within 24 hours of signing up so you can quickly take action on any suspicious or fraudulent activity.



Minimize the impact of identity theft:

In the event that your personal information is stolen and used, have peace of mind knowing that OnAlert can help you quickly. With full-service restoration services, you can call a US-based expert for assistance in restoring your identity.



Morgan Lewis

Gregory T. Parks

Partner
215.963.5170
gregory.parks@morganlewis.com

October 16, 2023

VIA EMAIL TO IDTHEFT@OAG.STATE.MD.US

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

Re: Updated Notice of Data Security Incident of Progress Software as Vendor to Fidelity National Information Services, Inc. and Community Trust Bank, Inc.

Dear Office of the Attorney General:

This Firm represents Fidelity National Information Services, Inc. ("FIS") and we are writing to update your office on behalf of FIS and its client, Community Trust Bank, Inc. ("CTBI"), regarding a notification submitted to your office on September 8, 2023 about a recent data security incident involving the secure file transfer software tool MOVEit Transfer provided by third-party vendor Progress Software.

Upon further review of the impacted files, FIS and CTBI determined on September 11, 2023 there were an additional 6 Maryland residents whose name, date of birth, Social Security number and/or bank account information among those files taken. Although there continues to be no indication that the disclosed personal information has been used for any fraudulent purpose, CTBI is sending notifications by mail to these recently identified individuals to explain what happened, what information was involved, what they and FIS have done, and how affected individuals can contact CTBI with questions. FIS and CTBI are offering two years of credit monitoring to affected customers of CTBI.

FIS carefully evaluates the cybersecurity posture of third-party file transfer tools, and FIS will continue this effort. FIS is also taking steps to further secure its use of all third-party transfer tools.

Further information about what FIS and CTBI have done and are recommending to the individuals in question can be found in the enclosed notifications that CTBI is sending to 6 additional Maryland residents via mail dated October 12, 2023.

Morgan, Lewis & Bockius LLP

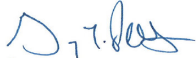
1701 Market Street
Philadelphia, PA 19103-2921
United States

 +1.215.963.5000
 +1.215.963.5001

State of Maryland
Office of the Attorney General
October 16, 2023
Page 2

If you have any questions, please feel free to contact me.

Regards,

A handwritten signature in blue ink, appearing to read "G. T. Parks", written in a cursive style.

Gregory T. Parks

Enclosure

October 12, 2023

RE: NOTICE OF DATA SECURITY EVENT

Dear Valued Customer:

We are writing to provide you with information regarding a recent third-party data incident which involves the security of some of your personal information. As such, we wanted to provide you with information about the incident, explain the services that are being made available to you, and let you know that we continue to take significant measures to protect your information.

What Happened

One of our service providers received notice from one of its third-party vendors, MOVEit, regarding a security vulnerability in the MOVEit Transfer solution which is utilized by our service provider to transmit data. MOVEit reported a zero-day vulnerability in MOVEit Transfer which has been actively exploited by unauthorized actors to gain access to data stored on the MOVEit server. MOVEit has acknowledged the vulnerability and has since provided patches to remediate the exploit. There was no compromise of our service provider's or our broader network security. The Bank's systems were not involved in this incident or compromised in any way.

What We Are Doing

Upon being informed of the vulnerability, our service provider immediately took actions to mitigate and assess the scope of information potentially compromised, including engaging third-party professionals to assist in the investigation and remediation of the vulnerability. Following our service provider's investigation, they discovered on July 24, 2023 that certain files that contain your personal information were accessed and potentially removed from the service provider's network by an unauthorized party on May 29-30, 2023. We were notified that your personal information may be involved on September 11, 2023. Our service provider is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident.

What Information Was Involved?

The information potentially accessible on the MOVEit server may have included your name, date of birth, Employee Identification Number and/or Social Security number, and/or bank account information.

What You Can Do

We have no evidence that any of your information has been used to commit financial fraud. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

To help protect your identity, our service provider is offering a complimentary 24-month membership to OnAlert™ (Essential Bundle) from ChexSystems®. OnAlert provides you with identity monitoring and can assist with the resolution of identity theft. **To activate your membership in OnAlert and start monitoring your personal information please enroll at <https://onalert.info/communitytrustbank> by December 31, 2023.** Your link will not work after this date. You will need to provide the website link noted above as proof of eligibility for this offer.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call the dedicated toll-free response line that has been set up to respond to questions at (833) 533-1790. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information.

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary 24 months Credit Monitoring**

For new member questions and assistance with enrollment, please contact the OnAlert customer care team at **(833) 919-4756**. A credit card is not required for enrollment into OnAlert. The response line is available Monday through Friday, 8:00 am to 10:00 pm CT, with Saturday and Sunday hours from 10:00 am to 7:00 pm CT.

With OnAlert (Essential Bundle), you will have access to the following features:

- **Single-Bureau Credit Report and Manual VantageScore® from Experian®:** Credit reports and scores from Experian.
- **Single-Bureau Credit Monitoring from Experian:** Actively monitors Experian files and alerts you of key changes and indicators of fraud.
- **Automatic VantageScore Tracker:** Shows you your credit score so you can see how lenders evaluate your creditworthiness.
- **VantageScore Simulator:** Interactive credit score simulator you can use to see how actions will potentially impact your Experian credit score.
- **Personalized Credit & Identity Alert Videos:** Credit and identity education videos.
- **Real Time Authorization Alerts:** Notifications of when your personal information is used for new applications or identity authorizations.
- **Dark Web Monitoring:** Internet and dark web surveillance monitoring of your personal information.
- **ChexSystems Monitoring and Alerts:** Actively monitors ChexSystems' database and alerts you of key activity and indicators of fraud. Chex Systems, Inc. (ChexSystems) is a nationwide specialty consumer reporting agency under the Fair Credit Reporting Act (FCRA).
- **Full-Service Restoration:** Certified Identity Theft Restoration Specialists available for assignment to help you address credit and non-credit related fraud.
- **Lost Wallet Assistance:** Protection of your personally identifiable information that has been compromised.
- **Up to \$1MM Identity Theft Insurance**:** Reimbursement for certain ancillary expenses associated with restoring your identity.

* Calculated on the VantageScore 3.0 model. Your VantageScore 3.0 from Experian® indicates your credit risk level and is not used by all lenders, so don't be surprised if your lender uses a score that's different from your VantageScore 3.0.

**The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. **Placing a Fraud Alert.**

Whether or not you choose to use the complimentary 24 month credit monitoring services, we recommend that you place an initial one (1) year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file at no cost. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. 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 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC

about fraud alerts and security freezes.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, <https://oag.dc.gov/consumer-protection>, Telephone: 202-442-9828.

Community Trust Bank, Inc.
346 North Mayo Trail
Pikeville, KY 41501

Estate of:

October 12, 2023

RE: NOTICE OF DATA SECURITY EVENT

Dear Estate of Valued Customer:

We are writing to provide you with information regarding a recent third-party data incident which involves the security of some of your loved one's personal information. As such, we wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your loved one's information.

What Happened

One of our service providers received notice from one of its third-party vendors, MOVEit, regarding a security vulnerability in the MOVEit Transfer solution which is utilized by our service provider to transmit data. MOVEit reported a zero-day vulnerability in MOVEit Transfer which has been actively exploited by unauthorized actors to gain access to data stored on the MOVEit server. MOVEit has acknowledged the vulnerability and has since provided patches to remediate the exploit. There was no compromise of our service provider's or our broader network security. The Bank's systems were not involved in this incident or compromised in any way.

What We Are Doing

Upon being informed of the vulnerability, our service provider immediately took actions to mitigate and assess the scope of information potentially compromised, including engaging third-party professionals to assist in the investigation and remediation of the vulnerability. Following our service provider's investigation, they discovered on July 24, 2023 that certain files that contain your loved one's personal information were accessed and potentially removed from the service provider's network by an unauthorized party on May 29-30, 2023. We were notified that your personal information may be involved on September 11, 2023. Our service provider is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident.

What Information Was Involved?

The information potentially accessible on the MOVEit server may have included your name, date of birth, Employee Identification Number and/or Social Security number, and/or bank account information.

What You Can Do

We have no evidence that any of your loved one's information has been used to commit financial fraud. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

This letter also provides other precautionary measures you can take to protect your loved one's personal information. Additionally, you should always remain vigilant in reviewing your loved one's financial account

statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your loved one's personal information.

If you have any further questions regarding this incident, please call the dedicated toll-free response line that has been set up to respond to questions at (606) 437-3282. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your loved one's information.

– OTHER IMPORTANT INFORMATION –

1) Protecting Deceased Individuals

The following steps are recommended for all deaths, regardless of age. It is best to notify all entities by telephone but such notifications **must** be followed-up in writing. Mail all correspondence certified, return receipt requested. Keep photocopies of all correspondence, including letters that you send.

- a) Obtain at least 12 copies of the official death certificate when it becomes available. In some cases you will be able to use a photocopy, but some businesses will request an original death certificate. Since many death records are public, a business may require more than just a death certificate as proof.
- b) Immediately contact the Credit Reporting Agencies (“CRAs”) in writing and request a “deceased” alert be placed on their credit report. You should also request a copy of the credit report.
- c) Contact all credit issuers, collection agencies, the CRAs and any other financial institutions that need to know of the death using the required procedures for each one. Include the following information on all letters:
 - Name and SSN of deceased
 - Last known address
 - Last 5 years of addresses
 - Date of birth
 - Date of death
 - To speed up processing, include all requested documentation specific to that agency in the first letter.
 - Send all mail certified, return receipt requested.
 - Keep copies of all correspondence, noting date sent and any response(s) you receive.
 - Contact each of the CRAs. Request a copy of the decedent’s credit report. A review of each report will let you know of any active credit accounts that still need to be closed, or any pending collection notices. Be sure to ask for all contact information on accounts currently open in the name of the deceased (credit granters, collection agencies, etc.) so that you can follow through with those entities.
 - Request that the report is flagged with the following alert: *“Deceased. **Do not** issue credit. If an application is made for credit, notify the following person(s) immediately: (list the next surviving relative, executor/trustee of the estate and/or local law enforcement agency- noting the relationship).”*
 - Friends, neighbors or distant relatives do not have the same rights as a spouse or executor of the estate. They are classified as a third party and a CRA may not mail out a credit report or change data on a consumer file upon their request. If you fall into this classification and are dealing with a very unique situation, you may write to the CRA and explain the situation. They are handled on a case-by case basis.

Specific instructions for each credit reporting agency (CRA) are listed below.

2) Specific Instructions from the 3 Credit Reporting Agencies

Experian

P.O. Box 9701
Allen, TX 75013

Ordering reports

- A spouse can obtain a credit report by simply making the request through the regular channels - mail, phone and Internet. The spouse is legally entitled to the report.
- The executor of the estate can obtain a credit report but must write Experian with a specific request, a copy of the executor paperwork and the death certificate.

Requesting changes or voicing concerns

- A spouse or executor may change the file to show the person as deceased via written request. A copy of the death certificate and in the case of the executor, the executor's paperwork must be included with the request.
- After any changes, Experian will send an updated credit report to the spouse or executor for confirmation that a deceased statement has been added to the credit report. This is important as executors and spouse can request other types of "changes" that we may not be able to honor.
- If ID Theft is a stated concern, Experian will add a security alert after the file has been changed to reflect the person as deceased.
- If there are additional concerns, Experian will add a general statement to the file at the direction of the spouse/executor. The spouse/executor must state specifically what they want the general statement to say, such as "Do not issue credit."

Equifax

P.O. Box 105139
Atlanta, GA 30348

To order a credit report

Equifax requests that the spouse, attorney or executor of the estate submit a written request to receive a copy of the deceased consumer's file. The request should include the following:

A copy of a notarized document stating that the requestor is authorized to handle the deceased consumer's affairs (i.e.: Order from a Probate Court or Letter of Testamentary)

For requests or changes

Equifax requests that a spouse, attorney or executor of the estate submit a written request if they would like to place a deceased indicator on the deceased consumer's file. The written request should include a copy of the consumer's death certificate. The request should be sent to the address listed above.

Upon receipt of the death certificate, Equifax will attempt to locate a file for the deceased consumer and place a death notice on the consumer's file. In addition, Equifax will place a seven year promotional block on the deceased consumer's file. Once Equifax's research is complete, they will send a response back to the spouse, attorney, or executor of the estate.

TransUnion (TU)
P.O. Box 2000
Chester, PA 19016

Ordering reports

- TU requires proof of a power of attorney, executor of estate, conservatorship or other legal document giving the requestor the legal right to obtain a copy of the decedent's credit file.
- If the requestor was married to the deceased and the address for which the credit file is being mailed to is contained on the decedent's credit file, then TU will mail a credit file to the surviving spouse.
- If the deceased is a loved one of the requestor, TU will mail a credit file to the parent upon receipt of a copy of the birth certificate or death certificate naming the parent as requestor.

Requesting changes or voicing concerns

- Placing a "decease alert" on reports: TU will accept a request to place a temporary alert on the credit file of a deceased individual from any consumer who makes such a request and identifies themselves as having a right to do so.
- The requestor's phone number is added to the temporary, three month alert. Upon receipt of a verifiable death certificate, TU will entirely suppress the decedent's credit file and so note it as a deceased consumer.
- TU will not mail out a copy of its contents without the requirements mentioned above.

If you suspect fraud, TU suggests a call to their fraud unit at 800-680-7289. It will place the temporary alert over the phone and advise the requestor of what needs to be sent to suppress the credit file and to disclose a copy of its contents. Requests can also be emailed to fvad@transunion.com.

3) Steps to take if you (surviving spouse or estate executor) suspect that someone is fraudulently using the information of a deceased person:

- a) Request a copy of the decedent's credit report as outlined above.
- b) Place a "deceased alert" on the report as outlined above.
- c) Notify the police in the decedent's jurisdiction if you have evidence of fraud (collection notice, bills, credit report). A suspicion (especially of identity theft by a family member) is best when backed with concrete evidence.
- d) Notify any creditor, collection agency, credit issuer, utility company that the person is deceased and date of death. Be sure to include a copy of the death certificate. Request an immediate investigation and that they contact you with the results of the investigation. Insist on letters of clearance, which you should keep with the other estate papers.
- e) In the event that the thief is a family member or relative, if the family is unable to decide on a course of action, it may be best to seek the advice of an attorney that specializes in estate or family law.