Alexander Walker
Office: 267-930-4801
Fax: 267-930-4771
Email: awalker@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

November 7, 2018

VIA EMAIL

Office of the Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188
Email: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir/Madam:

We represent Unified Trust Company, N.A. ("UTC"), 2353 Alexandria Drive, Suite 100, Lexington, KY 40504, and write to provide notice to your office of an incident that may affect the security of personal information relating to certain Washington residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, UTC does not waive any rights or defenses regarding the applicability of Washington law, the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about February 13, 2018, UTC became aware of suspicious activity within a UTC employee's email account. Upon learning of this suspicious email activity, UTC promptly launched an internal investigation, with the assistance of third-party forensic investigators. Through this investigation, on or about August 1, 2018, UTC confirmed that there was unauthorized access to two UTC email accounts between December 6, 2017 and February 25, 2018.

On or about October 1, 2018, as the result of a thorough review of the potentially exposed contents of the two email accounts, the investigation confirmed the population of potentially impacted individuals. The types of personal information potentially impacted in relation to this incident include the following: name, date of birth, address, Social Security number, and, for some, financial account number. Beginning on October 1, 2018, UTC took steps to identify the address information necessary for providing notification to the affected individuals.

Notice to Washington Residents

On November 7, 2018, UTC began mailing written notice of this incident to the affected individuals, including one thousand one hundred ninety-six (1,196) Washington residents. Written notice will be provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and to Be Taken

Upon discovering this incident, UTC promptly began an investigation with the assistance of a third-party computer forensics expert to determine the nature and scope of this incident, including identifying the individuals who may be affected, putting in place resources to assist them, and providing them with notice of this incident. UTC identified and mitigated the issue by ensuring that passwords for the affected email accounts were changed. UTC has also taken additional actions to strengthen the security of their email systems, including implementing multi-factor authentication and enhanced security procedures around client accounts, as well as providing additional training to users on how to identify phishing scams.

UTC is providing potentially affected individuals access to 12 months of credit monitoring and identity restoration services, through AllClear ID. Additionally, UTC is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

UTC reported this incident to, and has been cooperating with, their primary federal regulator, the Office for the Comptroller of the Currency (the "OCC"). UTC is also notifying other state regulators and the consumer reporting agencies, as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4801.

Very truly yours,

Alexander Walker of
MULLEN COUGHLIN LLC

ATW/anm

EXHIBIT A

unified trust

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

00001
R83050B

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

November 7, 2018

Re: Notice of Data Breach

Dear John Sample:

Unified Trust Company ("Unified Trust") recently discovered an incident that may affect the security of your personal information. We write to provide you with information about the incident, steps we are taking in response, and steps you can take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On or about February 13, 2018, Unified Trust became aware of suspicious activity within a Unified Trust employee's email account. Upon learning of this suspicious email activity, Unified Trust promptly launched an internal investigation, with the assistance of third-party forensic investigators. Through this investigation, on or about August 1, 2018, Unified Trust confirmed that there was unauthorized access to two Unified Trust email accounts between February 12, 2018 and February 13, 2018.

What Information Was Involved? On or about October 1, 2018, Unified Trust confirmed that the impacted email accounts contained, and the unauthorized actor had access to, personal information related to you, including: [redacted]. Unified Trust is unaware of any attempted or actual misuse of personal information contained within the affected accounts as a result of this incident.

What Are We Doing? We take very seriously this incident and the security of your personal information. Unified Trust identified and mitigated the issue by ensuring that passwords for the affected email accounts were changed. We have also taken additional actions to strengthen the security of our email systems, including implementing multi-factor authentication and enhanced security procedures around client accounts, as well as providing additional training to users on how to identify phishing scams. We continue to monitor our systems to protect the privacy and security of your personal information.

We are providing you with information you can use to better protect against identity theft and fraud, as well as access to 12 months of complimentary credit monitoring and identity restoration services with AllClear ID. Instructions for enrolling in the credit monitoring services, as well additional information on how to better protect against identity theft or fraud, are included in the attached *Privacy Safeguards*.

What Can You Do? You can review the *Privacy Safeguards* for additional information on how to better protect against identity theft and fraud. You can also enroll to receive the complimentary credit monitoring and identity restoration services described above.

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 1-855-683-1170. This toll-free line is available Monday through Saturday from 8:00 am to 8:00 pm CDT, excluding major national holidays. We apologize for any inconvenience or concern this incident causes you.

Sincerely,

Christina Crawford
Chief Risk Officer

Enclosure

PRIVACY SAFEGUARDS

Enroll in Credit Monitoring. As an added precaution, we have arranged to have AllClear ID protect your identity for 12 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 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-683-1170 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 1-855-683-1170 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. We also encourage you to remain vigilant, for at least the next 12 to 24 months, against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. You should promptly report suspected identity theft to appropriate authorities.

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.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-800-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

For More Information. You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the 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); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be promptly reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

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

For North Carolina residents, North Carolina residents may wish to review information provided by the North Carolina Attorney General, Consumer Protection Division at www.ncdoj.gov, by calling 877-566-7226, or writing to 9001 Mail Services Center, Raleigh, NC 27699.

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 Rhode Island residents, the Rhode Island Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. Approximately fourteen (14) Rhode Island resident may be impacted by this incident. You have the right to file and obtain a police report if you ever experience identity theft or fraud. Please note that, in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim.