BakerHostetler

Baker&Hostetler LLP

1735 Market Street
Suite 3300
Philadelphia, PA 19103-7501

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Brian J. Craig
direct dial: 202.861.1662
bxcraig@bakerlaw.com

July 7, 2022

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

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

Re: Incident Notification

Dear Attorney General Frosh:

We are writing on behalf of our client, United Cumberland Bank, to notify you of a security incident.

United Cumberland Bank recently concluded an investigation into a security incident that caused certain devices in its network to become unavailable. United Cumberland Bank immediately began an investigation, a cybersecurity firm was engaged, and measures were taken to address the incident. Law enforcement was also notified. United Cumberland Bank learned that there was unauthorized access to the network between March 21, 2022 and March 27, 2022. During that time, the unauthorized party obtained files stored on the file server. United Cumberland Bank conducted a review of those files and, on June 16, 2022, determined that the files contained the name and financial account number of one Maryland resident.

On July 6, 2022, United Cumberland Bank is providing written notice via United States Postal Service mail to the Maryland resident whose information was involved in accordance with Md. Code Ann., Com. Law § 14-3504. A copy of the notification letter is enclosed.[1] United Cumberland Bank has encouraged the individual to remain vigilant and report any unauthorized activity to their

[1] This report does not waive United Cumberland Bank's objection that Maryland lacks personal jurisdiction over it related to any claims that may arise from this incident.

financial institution. United Cumberland Bank is also providing a toll-free phone number for letter recipients to call for further information about the incident.

To help further protect against an incident like this, United Cumberland Bank is taking steps to further enhance the security of its network.

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

Sincerely,

Brian J. Craig

Brian J. Craig
Counsel

Enclosure

United Cumberland Bank

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name1>>:

United Cumberland Bank understands the importance of protecting the information we maintain. We are writing to inform you that we identified and addressed a security incident that involved some of your information. This notice explains the incident, the measures we have taken, and provides some additional steps you may consider taking.

We recently concluded an investigation into a security incident that caused certain devices in our network to become unavailable. We immediately began an investigation, a cybersecurity firm was engaged, and measures were taken to address the incident. We also notified law enforcement.

We learned that there was unauthorized access to our network between March 21, 2022 and March 27, 2022. During that time, the unauthorized party obtained files stored on our file server. We conducted a review of those files and, on June 16, 2022, determined that the files contained some of your information, including your name and << data elements>>.

<<IF AG791 - Adult CM>>
We wanted to notify you of this incident and to assure you that we take it seriously. As a precaution, we have arranged for you to receive a complimentary <<CM Length>> month membership to TransUnion's® *my*TrueIdentity credit monitoring service. This product helps detect possible misuse of your information and provides you with identity protection services focused on immediate identification and resolution of identity theft. *my*TrueIdentity is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and *my*TrueIdentity, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the additional information provided in this letter.

<<IF AG794 - Adult No CM>>
We wanted to notify you of this incident and to assure you that we take it seriously. We encourage you to remain vigilant by reviewing your financial statements for any unauthorized activity. You should immediately report any unauthorized activity to your financial institution. For more information on identity theft prevention and steps you can take to protect your information, please see the additional information provided in this letter.

We regret that this occurred and apologize for any inconvenience. To help prevent something like this from happening again, we are taking steps to further enhance the security of our network. If you have additional questions, please call 844-558-0788, Monday through Friday, between 9:00 a.m. and 9:00 p.m., Eastern Time.

Sincerely,

Michael Laxton

Michael Laxton
President / CEO

<<IF AG791 - Adult CM, map this page. If not, leave it out>>

TransUnion

Activation Code: <<Activation Code>>

3-Bureau Credit Monitoring Product Offering: (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online 3-bureau credit monitoring service (*my*TrueIdentity) for <<CM Length>> months provided by TransUnionInteractive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and inthe space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code **<< Activation Code>>** and follow the three steps to receive your creditmonitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, 3-bureau credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<< Engagement Number >>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain <<CM Length>> months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily 3- bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian® and Equifax®, including fraud alerts, new inquiries, new accounts, new publicrecords, late payments, change of address and more. The service also includes the ability to lock andunlock your TransUnion credit report online, access to identity restoration services that provide assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online 3-Bureau Credit Monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit files at TransUnion®, Experian® and Equifax®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12-24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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 bureau will provide you with 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.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

United Cumberland Bank's mailing address is 47 S Main Street, Whitley City, KY 42653 and phone number is (606) 376-0036.

Additional information for residents of the following states:

<<IF AG794 - Adult No CM, add:>>
Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

<<IF AG794 - Adult No CM, add:>>
West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.