BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Patrick H. Haggerty
direct dial: 513.929.3412
phaggerty@bakerlaw.com

July 6, 2021

VIA E-MAIL (DOJ-CPB@DOJ.NH.GOV)

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, UniBank, to notify your office of a security incident. UniBank is a full-service bank, headquartered in Lynnwood, Washington.

On June 9, 2021, UniBank experienced a theft that included an electronic device among the items stolen. Based on UniBank's investigation, the accessible data included information stored by the bank between the dates of March 1, 2021 through May 28, 2021. Upon learning about the theft, UniBank immediately notified law enforcement and federal regulators. UniBank has not found any evidence that this incident resulted in any unauthorized access to or use of any of the bank's internal computer systems or network, or in any customer information being affected. Out of an abundance of caution, UniBank conducted a review of the data that was potentially accessible from the stolen device and determined that information included the names, Social Security numbers, and/or driver's license or state identification numbers of two New Hampshire residents.

Beginning today, July 6, 2021, UniBank is mailing notification letters via U.S. mail to the two New Hampshire residents whose information may have been involved in the incident. A copy of the notification letter is enclosed. UniBank is offering a one-year membership in complimentary credit monitoring and identity protection services through Kroll. UniBank also has established a dedicated call center that individuals can call with questions about the incident or enrolling in credit monitoring.

To reduce the risk of a similar incident occurring in the future, UniBank is reviewing the security processes and procedures regarding its electronic devices.

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

Sincerely,

Patrick H. Haggerty
Partner

Enclosure

19315 Hwy 99, Lynnwood, WA 98036
www.unibankusa.com

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you about a data security incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you may consider taking in response. We sincerely regret any inconvenience this may cause you.

What Happened
On June 9, 2021, we experienced a theft that included an electronic device among the items stolen. Based on our investigation, the accessible data included information stored by the bank between the dates of March 1, 2021 through May 28, 2021. It appears that you were one of the individuals whose information was potentially accessible. We immediately notified law enforcement and federal regulators. At this time, we have not found any evidence that this incident resulted in any unauthorized access to or use of any of the bank's internal computer systems or network, or in any customer information being affected.

What Information Was Involved
We conducted a review of the data that was potentially accessible from the stolen device and we determined that the information included your <<b2b_text_1(ImpactedData)>>. Please note that at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing
Out of an abundance of caution, we have arranged to provide identity monitoring at no cost to you for one year through Kroll, a leader in risk mitigation and response. Kroll's team has extensive experience helping people who have sustained an unintentional exposure of confidential data. The identity monitoring services we are making available to you include Credit Monitoring, Fraud Consultation and Identity Theft Restoration. For more information on how to help safeguard your identity and Kroll Identity Monitoring, including instructions on how to activate your complimentary membership, please visit the below website and see the additional information provided with this letter.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **October 4, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

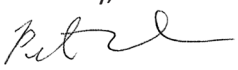
To prevent incidents like this from occurring in the future, we are reviewing our security processes and procedures regarding our electronic devices.

What You Can Do
In addition to activating in the identity monitoring services available to you, please see the information included in the "Additional Steps You Can Take" section of this letter which provides helpful tips and guidance.

For More Information
We have established a dedicated toll-free hotline to help answer questions you may have about the incident. Our representatives are available at 1-855-731-3352 for English, Monday through Friday, between 6:00 a.m. and 3:30 p.m. Pacific Time and 1-800-940-9698 for Korean, Monday through Friday, between 9:00 a.m. and 4:00 p.m. Pacific Time, excluding some U.S. holidays.

We deeply regret that this incident occurred and sincerely apologize for any concern or inconvenience this incident may cause.

Sincerely,



Peter R. Park
President & Chief Executive Officer

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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 to 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 you 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), www.ftc.gov/idtheft

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. This makes it more difficult for identity thieves to open new accounts in your name 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 on your credit reports. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions on how to place a security freeze on your credit reports, 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 when requesting a freeze. 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 receiving 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.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

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

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.