

## Appendix

In late September, United Bank experienced a cybersecurity incident that disrupted its business operations. United Bank's team promptly secured the network, began an investigation, and a computer forensics firm was engaged to assist. The investigation determined that an unauthorized actor gained access to some network servers, and specifically to files that may contain some personal information of nine Maine residents, including their name and Social Security number. The unauthorized actor did not access the core account system, where customer account data and balances are maintained. All customer personal accounts remained secure throughout the incident. United Bank confirmed the unauthorized actor deleted the files copied from its systems, and has no reason to believe any customer information has been misused.

On February 24, 2021, United Bank began mailing written notifications to those individuals whose information may have been involved, including nine Maine residents who are being notified of the incident in writing, in accordance with Me. Rev. Stat. Tit. 10, §1348.<sup>1</sup> A sample letter is attached. United Bank is offering eligible individuals complimentary credit monitoring, fraud consultation, and identity theft restoration services through Kroll for one year. United Bank will also recommend all notified individuals remain vigilant to the possibility of fraud by reviewing their financial account statements for unauthorized activity.

United Bank has established a toll-free number where all notified individuals can obtain further information regarding this incident. To prevent similar future incidents, United Bank implemented new password protocols, limited external email access, blocked access to malicious sites and IP addresses identified, and increased monitoring of network activity. United Bank also continues to educate its employees on how to identify and avoid malicious emails and have added new authentication measures for remote email access.

---

<sup>1</sup> This notice does not waive United Bank's objection that Maine lacks personal jurisdiction over United Bank regarding any claims related to this incident.



<<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>>,

United Bank understands the importance of securing and protecting our customers' personal and private information. Regrettably, we are writing to inform you of an incident that involves some of your information. This letter explains the incident, the measures we have taken, and the steps you may consider taking in response.

In late September, we experienced a cybersecurity incident that disrupted our business operations. Our team promptly secured the network, began an investigation, and a computer forensics firm was engaged to assist. The investigation determined that an unauthorized actor gained access to some network servers, and specifically to files that may have contained your <<b2b\_text\_1(DataElements)>>. The unauthorized actor did not access the core account system, where your individual account data and balances are maintained. Your personal account(s) remained secure throughout the incident.

We confirmed the unauthorized actor deleted the files copied from its system, and have no reason to believe any of your information has been misused. But as a precaution, United Bank is offering access to Kroll's complimentary identity monitoring services for one year. This service helps detect possible misuse of your personal information and provides notification, consultation, and restoration services in the event of identity theft. This service is completely free to you and activating this program will not hurt your credit score.

Follow these instructions to activate your free identity monitoring service:

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

*You have until **May 11, 2021** to activate your identity monitoring services.*

Your Membership Number: <<Member ID>>

Look further in this letter for additional steps you can take to help protect your personal and private information. We encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity and report any such activity to us. We provide free services such as online banking and text balance alerts to give you real time updates on your United Bank accounts.

We deeply regret any inconvenience or concern this incident may cause you. To help prevent something like this from happening in the future, we implemented new password protocols, limited external email access, blocked access to malicious sites and IP addresses identified, and increased monitoring of network activity. We continue to educate our employees on how to identify and avoid malicious emails and have added new authentication measures for remote email access. United Bank is a stronger, more secure company having gone through this experience.

United Bank has partnered with Kroll's experts to provide support throughout this process. Their agents are available at 1-855-763-1132, Monday through Friday, between 8:00 a.m. and 5:30 p.m. Central Time.

Sincerely,

A handwritten signature in black ink, appearing to read "James J. Edwards, Jr.", written in a cursive style.

James J. Edwards, Jr.  
CEO

## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

### Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—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.

## ADDITIONAL STEPS YOU CAN TAKE

We advise you 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](http://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](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://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), [www.ftc.gov/idtheft](http://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.

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.

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](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://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.