

## Appendix

On October 7, 2020, Parkway concluded its investigation of an incident that involved the unauthorized access to and encryption by ransomware of certain devices on the Parkway network. Upon first identifying the security incident Parkway immediately launched an investigation with the assistance of an outside cybersecurity firm and took measures to address the incident and restore operations.

Through the investigation Parkway learned that an unauthorized party gained access to the Parkway network between the dates of July 23, 2020 and August 20, 2020. The investigation identified unauthorized access to files stored on Parkway's servers and was unable to rule out the possibility that the unauthorized party viewed the materials. Parkway conducted a comprehensive review of the materials on the affected devices and determined that the personal information of one Maine resident was in the materials including the individual's name, address, Social Security number and banking information.

Beginning on November 3, 2020, Parkway will mail a notification letter via U.S. mail to the Maine resident whose personal information may have been involved in this incident, in accordance with Me. Rev. Stat. Tit. 10, §1348.<sup>1</sup> A copy of the notification letter is enclosed. Parkway is offering one year of complimentary credit monitoring and identity theft protection service through Experian to the affected individual. Parkway is also providing a call center for the individuals to call with questions regarding the incident.

To help prevent a similar incident from occurring in the future, Parkway has implemented additional security measures to enhance the security of its network, including deploying an endpoint threat detection and response tool.

---

<sup>1</sup> This notice is not, and does not constitute, a waiver of Parkway's objection that Maine lacks personal jurisdiction over it regarding any claims related to this data security incident.

Parkway Products, LLC  
Mail Handling Services  
777 E Park Dr  
Harrisburg, PA 17111



[REDACTED]

October 30, 2020

Dear [REDACTED],

Parkway Products, LLC (“Parkway”) understands the importance of protecting the information we maintain. We are writing to inform you about an incident that involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

On August 19, 2020, Parkway identified a security incident that resulted in data on certain devices becoming encrypted by ransomware. Parkway immediately began to investigate, a cybersecurity firm was engaged, and measures were taken to address the incident and restore operations. The investigation identified that there was unauthorized access to files stored on Parkway’s servers.

Parkway completed a careful review of its file servers to determine what information may have been accessed without authorization. On October 7, 2020, we determined that the information on the servers included information about Parkway’s current and former employees, as well as their spouses and dependents (if they participated in Parkway’s health plan), as well as employees of certain companies acquired by Parkway. The information in the files includes names, addresses, dates of birth, Social Security numbers, and banking information. The files may also include health insurance information.

We wanted to notify you of this incident and assure you that we take it very seriously. It is always advisable to remain vigilant for signs of unauthorized activity by reviewing your financial account statements, health insurance statements and explanation of benefits statements. If you see charges or activity you did not authorize, we suggest that you contact the provider immediately. As a precaution, we have secured the services of Experian® to offer you a complimentary one-year membership to Experian’s IdentityWorks<sup>SM</sup>. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is completely free and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect yourself, please see the pages that follow this letter.**

Parkway regrets that this occurred and apologizes for any inconvenience. We have already implemented additional security measures to enhance the security of our network, including deploying an endpoint threat detection and response tool. If you have additional questions, please call the dedicated call center established for this matter at 888-919-9910, Monday through Friday, between 8:00 a.m. and 5:00 p.m., Eastern Time.

Sincerely,

A handwritten signature in black ink, appearing to read "Amber Galford".

**Amber Galford**  
**Director, Human Resources**

## EXPERIAN CREDIT MONITORING ENROLLMENT INSTRUCTIONS

To help protect your identity, we are offering a **complimentary one-year membership** of Experian IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

### **Activate IdentityWorks Credit 3B Now in Three Easy Steps**

1. ENROLL by: **January 26, 2021** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [REDACTED]
3. PROVIDE the **Activation Code**: [REDACTED]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [NUMBER]. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

### **ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:**

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE<sup>TM</sup>:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance<sup>\*\*</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit> or call [877-288-8057](tel:877-288-8057) to register with the activation code above.**

**What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration) for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [877-288-8057](tel:877-288-8057).

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* 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.

## 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. 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:** 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](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.

We also recommend that you review any statements that you receive from your health insurer or healthcare providers. If you see services that you did not receive, please contact the insurer or provider immediately.

**Additional information for residents of the following states:**

**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](http://www.ncdoj.gov)