

March 2, 2022

Anjali C Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Email: IDTheft@oag.state.md.us

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

Re: Data Security Incident
Client: Parkline, Inc.
File No.: 15991.01195

Dear Attorney General Frosh:

We represent Parkline, Inc. (“Parkline”), a manufacturing company operating out of West Virginia and Texas in regards to a recent data security incident. Parkline takes this matter very seriously and is taking measures to remediate the incident and provide notice to potentially affected individuals.

This letter will serve to inform you of the nature of the incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that Parkline has taken in response to the incident.

1. Nature of the incident.

On February 2, 2022, Parkline discovered that current and former employee information stored in a folder on our network with restricted access may have been accessible to unauthorized employees. Parkline promptly took steps to mitigate exposure by removing the folder from the network and updating the access control policy for that folder. Additionally, Parkline commenced an investigation and engaged third party cybersecurity experts to determine the nature and scope of the incident. The investigation revealed that Parkline employees who were not authorized to access this folder may have had access. There is no evidence that all employee information stored in the folder was in fact accessed, viewed, taken, or misused. Nor is there evidence that anyone outside of current Parkline employees could have accessed this folder. Immediately after concluding its review, Parkline procured credit monitoring for affected individuals and drafted notices to individuals and state and federal regulators as appropriate.

The investigation revealed that the exposed file contained the following types of personal information. PII impacted includes name, date of birth, Social Security number, Driver’s License number, Passport number, and/or financial account information.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

2. Number of Maryland residents affected.

Parkline discovered that one (1) resident of Maryland was impacted by this incident. A notification letter was sent to these individuals on March 3, 2022. A sample notice letter that was sent to the impacted individuals is included as **Exhibit A**.

3. Steps taken.

Parkline takes the security of personal information in its control very seriously, and has taken steps to prevent a similar event from occurring in the future, including but not limited to: reviewing and modifying the internal access control policies and procedures to strengthen access rights to sensitive data, increasing the strength of account authentication processes, reviewing and updating current data inventory management policies to better protect sensitive data, and adding encryption of data-at-rest capabilities to hardware storing information on the network.

Parkline has also provided 12 months of credit monitoring, dark web monitoring, and identity theft protection services to the individuals whose PII was impacted.

4. Contact information.

Parkline remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

Enclosure

EXHIBIT A



<Individual>
<Address 1>
<Address 2>

March 3, 2022

Notice of Data Security Incident

Dear <Individual>,

We are writing to inform you of a data security incident which affected Parkline, Inc. ("Parkline"), a U.S.-based building manufacturer operating out of West Virginia and Texas. The data security incident may have resulted in the potential compromise of some of your personal data. While we have no indication that your information has been misused, this letter contains information about the incident and information about how to protect your personal information going forward. Parkline considers the protection of sensitive information a top priority, and sincerely apologizes for any inconvenience as a result of the incident.

What Happened

On February 2, 2022, Parkline discovered that current and former employee information stored in a folder on our network with restricted access may have been accessible to unauthorized employees. Parkline promptly took steps to mitigate exposure by removing the folder from the network and updating the access control policy for that folder. Additionally, Parkline commenced an investigation and engaged third party cybersecurity experts to determine the nature and scope of the incident. The investigation revealed that Parkline employees who were not authorized to access this folder may have had access. There is no evidence that all employee information stored in the folder was in fact accessed, viewed, taken, or misused. Nor is there evidence that anyone outside of current Parkline employees could have accessed this folder. Nonetheless, **out of an abundance of caution, Parkline is providing notice to all employees and certain former employees with personal information in the folder, regardless of whether their information was in fact subject to unauthorized access or acquisition. At this time, Parkline has no reason to believe that any individual's information has been misused as a result of this event.**

What Information Was Involved

While we have no reason to believe that your information has been misused as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the unauthorized party may have had access to your name, date of birth, Social Security number, Driver's License number, Passport number, and/or financial account information. **Not every data element was present for every individual. Additionally, please note that the information did not include any individual's credit card or debit card numbers.**

What We Are Doing

The security and privacy of your personal information contained within Parkline's internal network is a top priority, and Parkline is taking additional measures to protect this information. Since the incident, Parkline has continued to strengthen their security posture by reviewing and modifying the internal access control

policies and procedures to strengthen access rights to sensitive data, increasing the strength of account authentication processes, reviewing and updating current data inventory management policies to better protect sensitive data, and adding encryption of data-at-rest capabilities to hardware storing information on the network.

We are also providing you with 12 months of complimentary credit monitoring, dark web monitoring, and up to \$1,000,000 in identity theft protection. Parkline strongly encourages you to take advantage of these services. More information on how to sign up for the services can be found below.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file.

Please review the enclosed *Additional Important Information*, to learn more about how to protect against the possibility of information misuse.

The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause. If you have any questions, please do not hesitate to call 1-800-405-6108 Monday through Friday, between 8:00 AM and 8:00 PM, Eastern time.

Sincerely,

A handwritten signature in black ink that reads "Bill Estep". The signature is fluid and cursive, with a long horizontal line extending from the end of the name.

Bill Estep
President, Parkline, Inc.

Credit Monitoring

We are providing you with access to **Single Bureau Credit Monitoring** services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by Cyberscout, a company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **<https://www.myidmanager.com>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **107beu7gjc99**. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

The enrollment requires an internet connection and an email account, and services may not be available to minors under the age of 18 years of age. When signing up for monitoring services, you may be asked to verify personal information for our own protection to confirm your identity.

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 <https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fair Credit Reporting Act: You are also advised that you may have additional rights under the federal Fair Credit Reporting Act.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
[\(800\)-525-6285](tel:(800)525-6285)

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
[\(888\)-397-3742](tel:(888)397-3742)

www.experian.com/freeze

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022
[\(800\)-680-7289](tel:(800)680-7289)

freeze.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed above.