WILSON ELSER

WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

July 1, 2022

Ross M. Molina, Esq.
504.702.1726 (direct)
Ross.Molina@WilsonElser.com

SENT VIA U.S. MAIL

North Dakota Attorney General's Office
600 E. Boulevard Ave Dept. 125
Bismarck ND 58505
Attn: Data Security Breach Notification

Re:	**Our Client**	**:**	**Professional Finance Company, Inc.**
	Matter	**:**	**Data Security Incident on February 26, 2022**
	Wilson Elser File #	**:**	**16516.01782**

Dear Attorney General:

We represent Professional Finance Company, Inc. ("PFC"), which is located in Greeley, Colorado. Our representation of PFC relates to a data security incident described in more detail below. PFC takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security incident, the number of North Dakota residents being notified, what information has been compromised, and the steps that PFC has taken to restore the integrity of the system. We have also enclosed a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On February 26, 2022, PFC detected and stopped a sophisticated ransomware attack, in which an unauthorized third party accessed and disabled some of PFC's computer systems. PFC immediately engaged third-party forensic specialists to assist with securing the network environment and investigating the extent of any unauthorized activity. On March 28, 2022, the initial investigation determined that an unauthorized third party may have accessed certain individual personal information during this incident, including first and last name, address, accounts receivable balance and information regarding payments made to accounts, and, in some cases, date of birth, Social Security number, health insurance and medical treatment information. Notably, the impacted data **did not** include any medical records or any individual payment card, banking or financial information.

PFC continued the investigation to determine the scope of the incident, including identifying which individuals were potentially impacted. On or around May 5, 2022, PFC provided notice of the incident to its affected clients. Since that time, PFC has worked to provide its clients with lists of the potentially impacted individuals, prepare notification letters, perform a NCOA search to secure

272517686v.1

221502

updated addresses for each individual, and offer credit monitoring and protection services for each individual as well as implement a call center that will assist individuals with questions they may have regarding the incident and credit monitoring offering.

Notably, PFC is not aware of any evidence that personal information has been misused. PFC has not received any reports of related identity theft since the date of the incident (February 26, 2022 to present).

2. Number of North Dakota Residents Affected

At this time, a total of 778 residents of North Dakota have been identified as potentially affected by this security incident. Notification letters to these individuals were mailed on July 1, 2022, by first class mail. A sample copy of the notification letter is attached.

3. Steps Taken

Upon detecting this incident, PFC moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of the network environment. PFC wiped and rebuilt affected systems and have taken steps to bolster network security. PFC also reviewed and altered policies, procedures, and network security software relating to the security of systems and servers, as well as how PFC stores and manages data.

PFC offered free credit monitoring services to all potentially affected individuals.

4. Contact Information

PFC 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 Ross.Molina@WilsonElser.com or 504.702.1726.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Ross M. Molina

Copy: Robert Walker, Esq. (Wilson Elser LLP)

Enclosure: *Sample Notification Letter*

Professional Finance Company
c/o Cyberscout
38120 Amrhein Road
Livonia, MI 48150

[redacted]

Via First-Class Mail

July 1, 2022

Dear [redacted],

Professional Finance Company, Inc. ("PFC") provides accounts receivable management services to various organizations, including [redacted]. We are writing to inform you of an incident that involved your personal information. We take the security of your personal information seriously, and want to provide you with information and resources you can use to protect your information.

What Happened and What Information was Involved:

On February 26, 2022, we detected and stopped a sophisticated ransomware attack, in which an unauthorized third party accessed and disabled some of PFC's computer systems. We immediately engaged a third party forensic firm to assist us with securing the network environment and investigating the extent of any unauthorized activity. Our investigation determined an unauthorized third party accessed certain individual personal information during this incident. On May 5, 2022, PFC notified [redacted] of the incident and impacted data. Please be assured that this incident only impacted data on PFC's systems. Therefore, it did not involve [redacted]'s network or information systems.

We found no evidence that your information has been specifically misused; however, it is possible that the following information could have been accessed by an unauthorized third party: first and last name, address, accounts receivable balance and information regarding payments made to your account, social security number. Notably, your medical records and financial account or payment card information **were not** compromised as a result of this incident.

What We Are Doing:

Data security is one of our highest priorities. Upon detecting this incident we moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of our network environment. We wiped and rebuilt affected systems and have taken steps to bolster our network security. We also reviewed and altered our policies, procedures, and network security software relating to the security of our systems and servers, as well as how we store and manage data.

We value the safety of your personal information and are providing you with access to Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your 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 your identity is compromised. These services will be provided by Cyberscout, a leading data protection company.

What You Can Do:

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/PFC** and follow the instructions provided. When prompted, please provide the following unique code to receive services: [redacted]. Cyberscout is available Monday through Friday, 6:00am - 6:00pm MDT. Please note the deadline to enroll is October 3, 2022.

We encourage you to take full advantage of this service offering. Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your information

For More Information:

If you have additional questions, please call our dedicated, toll-free line at 1-844-663-3160, Monday through Friday, 6:00am - 6:00pm MDT.

Sincerely,
Professional Finance Company, Inc

Additional Information

Credit Reports: 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.

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	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 https://www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 https://www.transunion.com/credit-freeze

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 listed above.

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

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and https://ag.ny.gov/.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

For Vermont Residents, if you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).