

December 9, 2022

M. Mendel Epstein
212.915.5237 (direct)
Mendel.Epstein@wilsonelser.com

Via Email ID Theft@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: Cybersecurity Incident Involving RFI Security, Inc. dba RFI Communications

Dear Attorney General Frosh:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents RFI Security, Inc. dba RFI Communications (“RFI”), a security system supplier located at 360 Turtle Creek Ct, San Jose, CA 95125, with respect to a recent cybersecurity incident (hereinafter, the “Incident”). RFI takes the security and privacy of the information in its control very 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 Incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that RFI has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On or about February 18, 2022, RFI first discovered that its computer systems were impacted by a Ransomware incident, which may have resulted in the inadvertent exposure of personal information of current and former RFI customers and employees. RFI has since worked diligently to determine what happened and what information was involved as a result of this incident.

Although RFI is unaware of any fraudulent misuse of information, it is possible that individuals’ full names, addresses, dates of birth, drivers’ license numbers, and Social Security numbers may have been exposed as a result of this unauthorized activity.

As of this writing, RFI has not received any reports of related identity theft since the date of the incident.

2. Number of Maryland Residents Affected

RFI discovered that the Incident may have resulted in the unauthorized exposure of information pertaining to one (1) Maryland resident. A notification letter to this individual was mailed on December 6, 2022, by First Class Mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps Taken in Response to the Incident

RFI is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, RFI moved quickly to investigate and respond to the Incident, assessed and upgraded the security of its systems, and notified the FBI. Additionally, RFI engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Lastly, RFI engaged a third party data mining company and identified the potentially affected individuals in preparation for notice.

Although RFI is not aware of any actual or attempted misuse of the affected personal information, RFI offered twelve (12) months of complimentary credit monitoring and identity theft restoration services through Cyberscout to all individuals to help protect their identity. Additionally, RFI provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact Information

RFI 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 Mendel.Epstein@WilsonElser.com or (212) 915-5237.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

M. Mendel Epstein

M. Mendel Epstein

EXHIBIT A

RFI Enterprises, Inc.
c/o Cyberscout
P.O. Box 3923
Syracuse, NY 13220



VIA FIRST-CLASS MAIL

Nicholas P Lengyel
18915 Sarichef Loop
Eagle River, AK 99577-8629

December 6, 2022

Notice of Data Incident

Dear Nicholas Lengyel:

RFI recently experienced a data security incident which may have affected your personal information. We take the protection and proper use of your information seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and steps you can take to safeguard your information.

What Happened

On or about February 18, 2022, RFI Enterprises' computer systems were impacted by a Ransomware incident, which may have resulted in the inadvertent exposure of personal information of current and former RFI customers and employees. We have since worked diligently to determine what happened and what information was involved as a result of this incident.

What Information Was Involved

The elements of your personal information that were exposed may have included, and potentially were not limited to your: name, address, social security number, date of birth, and driver's license number. Please note that there is no evidence at this time that any of your personal information has been misused as a result of this incident.

What We Are Doing

We are working with cybersecurity counsel to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to strengthen our security posture to prevent a similar event from occurring again in the future. Out of an abundance of caution we are providing you with the following services:

RFI appointed representatives are available for ninety (90) days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern Time, Monday through Friday, excluding holidays. Should you have any questions, please call the help line 1-833-520-2062 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

* Services marked with an "*" require an internet connection and e-mail account and will require enrollment by parent or guardian first. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Additionally, 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 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 that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a company specializing in fraud assistance and remediation services.

What You Can Do

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/rfjenterprises> and follow the instructions provided. When prompted please provide the following unique code to receive services: **BGREME4PTU** In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter.

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. The FTC also provides information on-line at www.ftc.gov/idtheft.

We encourage you to remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following page, which contains important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call 1-833-520-2062 Monday – Friday, 8:00 am to 8:00 pm Eastern Time, excluding holidays.

Sincerely,

RFI

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:

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
equifax.com/personal/credit-report-services/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

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