JacksonLewis

Jackson Lewis P.C.
200 Connell Drive, Suite 200
Berkeley Heights NJ 07922
(908) 795-5200 Direct
(908) 464-2614 Fax
jacksonlewis.com
Richard J. Cino – Managing Principal

Mary T. Costigan, Esq.
Mary.costigan@jacksonlewis.com

July 28, 2021

Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301
Telephone: (603) 271-3658

Re: Data Security Incident

Dear Sir or Madam:

We represent Ferolie Corporation dba C.A. Ferolie ("Ferolie"), located at 2 Van Riper Road, Montvale, NJ 07645. Pursuant to the N.H. Rev. Stat. §§359-C:19 *et seq.*[1], we are writing to notify you of a data incident.

On June 10, 2021, Ferolie learned that it was the victim of a malware attack which may have resulted in the unauthorized access and acquisition of personal information of eight New Hampshire residents. Upon discovering the attack, Ferolie engaged a third-party cybersecurity firm to provide expert assistance with securing its systems, remediation efforts, and to perform a forensic investigation into the nature and scope of the incident. As part of these efforts, Ferolie has deployed enterprise-wide endpoint monitoring solutions to detect any continued presence of the threat actors in its systems. Ferolie is working diligently to identify how this incident occurred.

Ferolie will be providing the affected individuals with written notice on or about July 29, 2021. In addition to advising the individuals on measures they can take to protect themselves, it has arranged for twenty-four-months of complimentary Identity Protection Services which includes single bureau credit monitoring. Please see attached letter.

Ferolie continues to assess its security practices and will take step, as necessary, to minimize the risk of a similar incident occurring in the future. Should the company become aware of any significant developments concerning this situation, we will inform you.

[1] Please note that by providing this letter the Company is not agreeing to the jurisdiction of State of New Hampshire or waiving its right to challenge jurisdiction in any subsequent actions.

Please let us know if you have any questions.

Sincerely,
JACKSON LEWIS PC

s/Mary T. Costigan
Mary T. Costigan

Encl.

4848-5418-7505, v. 1

LETTERHEAD

Name
Address

Verification/Enrollment Code: [insert]

Date [insert]

Dear [Name]:

Notice of Data Breach

We are writing to notify you that we experienced a data incident that may have involved your personal information. In this letter, we describe what happened, how we are handling the incident, and who you can contact if you have any questions. At the end of this letter, we include precautionary measures you can take to protect yourself.

What Happened

On June 10, 2021, we learned that we were the victim of a malware attack that affected our company systems. Based on our preliminary investigation, it appears the incident may have begun in December 2020.

What Information Was Involved

Although the investigation is ongoing, data affected by the incident may include your name and Social Security Number.

What We Are Doing

Upon discovering the attack, we engaged a third-party cybersecurity expert to help with our remediation efforts and perform a forensic investigation into the nature and scope of the incident. As part of these efforts, we have deployed enterprise-wide endpoint monitoring solutions to detect any continued presence of the threat actors in our systems. We are working diligently to identify how this incident occurred. As we move through this process, we will continue to assess our security practices and take steps, as necessary, to minimize the risk of a similar incident occurring in the future.

At this time, we have no indication that your personal information has been used to commit identity theft. However, as an added precaution, we would like to offer you complimentary Identity Protection Services for two-years. These services include:

- Single Bureau Credit Monitoring: Monitoring of a single credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member' credit report, bankruptcies, court judgments

and tax liens, new addresses, new employers, and other activities that affect the member' credit record.

- CyberScan Dark Web Monitoring: Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.
- $1M Reimbursement Insurance: Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.
- Fully Managed Identity Recovery: IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage the restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

We encourage you to contact IDX with any questions and to enroll in free identity protection services. Please note the deadline to enroll is [Enrollment Deadline].

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be

assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

What You Can Do

In addition to enrolling in the complimentary ID theft protection and monitoring services, as with any data incident, we encourage you to remain vigilant and consider taking these precautionary measures:

- Review your personal account statements;
- Monitor free credit reports;
- Report any suspicious activity on your accounts to the company or financial institution; and
- Immediately report any fraudulent activity or suspected identity theft to your local law enforcement, state attorney general, and/or the Federal Trade Commission.

For More Information

We regret any concern this incident may cause you. Please call **[insert]** if you have any questions.

Sincerely,
Ferolie Corporation

_____
James L. Ferolie
Chief Information Officer

Additional Actions to Help Reduce Chances of Identity Theft

We recommend that you consider taking one or more of the following steps as a precautionary measure to avoid identity theft, obtain additional information, and protect your personal information:

1. **Place a 90-day fraud alert on your credit file**

An initial 90-day security alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the credit cannot verify that you have authorized this, the request should not be satisfied. You may contact any one of the credit reporting companies below for assistance.

Experian: 1-888-397-3742; www.experian.com
TransUnion: 1-800-680-7289; www.transunion.com
Equifax: 1-800-525-6285; www.equifax.com

2. Place a security freeze on your credit

If you are concerned about becoming a victim of security fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report, which will prevent them from extending credit. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also accessed through each of the credit reporting companies and there is no charge.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	Trans Union Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and

7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you have one.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and Social Security Number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and Social Security Number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

3. Order your free annual credit reports

Consider visiting www.annualcreditreport.com or call 877-322-8228 to order your free annual credit reports. Once you receive your credit reports, review them for discrepancies, identify any accounts you did not open, or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice any incorrect information, contact the credit reporting company.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 2390	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(866) 510-4211	(866) 751-1323	(800) 888-4213
psol@equifax.com	databreachinfo@experian.com	https://tudatabreach.tnwreports.com/
www.equifax.com	www.experian.com/	www.transunion.com

4. Manage your personal information

You can take steps that include carrying only essential documents with you, being aware of with whom you share your personal information, and shredding receipts, statements, and other sensitive information.

5. **Remove your name from mailing lists of pre-approved offers of credit for approximately six months.**

   By calling 1-888-567-8688, you can obtain a form to remove your name from pre-approved credit card offers. You will need to share some personal information, such as your name, Social Security Number and date of birth when you submit your request. For more information on opting out of prescreen offers of credit, please refer to: http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre17.shtm.

6. **Use Tools from Credit Providers**

   Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on your credit cards and bank accounts for notice of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, contact your creditor or bank immediately and file an identity theft report with your local police and contact a credit reporting company.

7. **Report suspected identity fraud**

   You can file a report of suspected incidents of identity theft with local law enforcement, your state Attorney General, or the Federal Trade Commission.

8. **To obtain additional information about identity theft and ways to protect yourself**

   Contact the Federal Trade Commission ("FTC") either by visiting www.ftc.gov, www.consumer.gov/idtheft, or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you can report this to the Fraud Department of the FTC, who will collect all information and make it available to law-enforcement agencies. Contact information for the FTC is: 877-436-4338, TTY 866-653-4261.

   Federal Trade Commission
   Consumer Response Center
   600 Pennsylvania Avenue
   NW Washington, DC 20580

   In addition to the FTC, you also may contact your state's attorney general's office and the credit reporting agencies above to provide you with information about fraud alerts and security freezes.