



ArentFox Schiff LLP

1717 K Street, NW
Washington, DC 20006

202.857.6000 **MAIN**
202.857.6395 **FAX**

afslaw.com

February 23, 2024

Reed Freeman

Partner

202.350.3610 **DIRECT**

reed.freeman@afslaw.com

Office of the Maine Attorney General

Attn: Security Breach Notification

6 State House Station

Augusta, ME 04333

Submitted as an Attachment to the Maine Security Breach Reporting Form

NOTICE OF DATA SECURITY BREACH

Dear Sir or Madame:

We serve as counsel for Crossroads Equipment Lease & Finance, LLC (“Crossroads”), located at 9385 Haven Ave., Rancho Cucamonga, CA 91730. This letter supplements the information we are providing via the Maine Security Breach Reporting Form.

Crossroads experienced a ransomware event on April 1, 2023, which resulted in a complete shutdown of its operations. Despite the significant time, work, and cost associated with this incident, as well as Crossroads’ significant efforts to restore its systems, Crossroads has still not fully recovered from it.

The attacker encrypted Crossroads’ servers and deleted Crossroad’s backup files. Throughout the month of April, the company worked with a vendor to acquire the decryption key to its servers. The key it ultimately obtained, however, was unsuccessful at fully decrypting Crossroads’ servers.

The company was then forced in May 2023 to try to restore the deleted backups to gain access to some portion of the lost company data and to fast-track an already in-progress implementation of a new customer-facing application. Crossroads also had to rebuild the LeaseComplete application from a backup that Crossroads received from Dominion Leasing Software, LLC (the LeaseComplete maker). Because some of Crossroads’ customer data resided on systems that were not accessible to the attacker, these restoration and recovery efforts allowed Crossroads to restore some of its operational files. The attacker did not have access to the Vision and LeaseComplete applications, which had been the primary systems that Crossroads used to process personal information, because those applications required different access credentials.

From the end of May until August 2023, Crossroads' sister company also restored its own data from recovered backup files, as a portion of its files also resided on encrypted systems. Through this process, Crossroads learned in August 2023 that some personal information pertaining to Crossroad's business might have existed in the encrypted systems. Upon learning this, Crossroads immediately reached out to a vendor to determine what personal information may have been compromised in this attack. However, in the course of due diligence with its insurance carrier, Crossroads learned of difficulties and technical limitations with that vendor. Crossroads therefore determined it was necessary to engage a different vendor to ensure the process of determining the nature and scope of personal information that may have been compromised was being done as well, and as quickly, as possible.

Crossroads engaged the new vendor for this purpose on October 23, 2023. Even still, Crossroads faced challenges getting access to the recovered data and making its recovered files available to the new vendor. This process took almost a month to complete. The vendor then went through its data mining process, and on January 25, 2024, it completed its work. It was at this time that Crossroads was aware of the nature and scope of the personal information that may have been compromised in this incident. Crossroads then asked us to prepare the appropriate notices.

While we have no evidence that personal information was misused, the personal information present in the computer systems accessed may have included:

- Name
- Mailing address
- Phone number, mobile and/or home
- Email address
- Date of birth
- Social Security number
- 1099 Forms
- Driver's license number, Passport number, or other state or government IDs (including photocopies of such)
- Vehicle information, such as Vehicle Identification Number or License Plate Number
- Tax documents, including Tax Returns and Tax Forms and individual taxpayer identification number
- Credit or Debit card numbers
- Bankruptcy filings
- Financial statements and financial account numbers plus a security code, access code, or password that may permit access the account
- Credit reports, including credit score and credit history
- Loan applications

- Medical information
- Digital signatures

Protecting the privacy and security of personal information is of critical importance to Crossroads. Crossroads is informing Maine residents of this incident because it respects their privacy. At this time, we are aware of four (4) Maine residents potentially affected by this incident. Each such resident will receive notification of this incident in a hard-copy letter via U.S. Mail dated February 23, 2024.

Crossroads has taken a number of steps to mitigate potential harm and remedy the incident. On April 3, 2023, Crossroads secured access to its systems and began migrating all data to a cloud server with enhanced security. The Federal Bureau of Investigation was notified of this incident on April 5, 2023.

Crossroads has put in place additional security controls to protect against future attacks. This includes enhanced security around access to our system requiring a second form of user verification (MFA), more complex user-restricted access, redundant backup of the data, continuous monitoring to protect against further incidents, and implemented additional technical and organizational controls.

Crossroads is offering affected residents two years of free credit monitoring through Experian.

Please contact me with questions about this matter.

Sincerely,

A handwritten signature in black ink that reads "Reed Freeman". The signature is written in a cursive, slightly slanted style.

Reed Freeman



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

K8982-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 CONSUMER ALL OTHER STATES
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



February 23, 2024

RE: NOTICE OF DATA SECURITY BREACH

Dear Crossroads Equipment Lease & Finance, LLC Customer:

We’re writing to you as a valued customer of Crossroads Equipment Lease & Finance, LLC (“Crossroads”) to inform you of a cybersecurity incident that affected our business and possibly your personal information. While we are unaware of any actual misuse of your information, we are providing notice to you about this incident because your privacy is of the utmost importance to us.

What Happened? On April 2, 2023, Crossroads became aware that its computer systems were subject to a ransomware attack. As part of the attack, Crossroads’s computer systems were encrypted, preventing Crossroads from accessing many of its digital files. This incident impacted Crossroads’s ability to complete ACH payments, as well as to perform other important business functions. On January 25, 2024, Crossroads became aware of the nature and scope of the personal information that may have been compromised.

When Did It Happen? The ransomware attack occurred on April 1, 2023.

What Information Was Involved? While we have no evidence that your personal information was acquired, the personal information present in the computer systems accessed may have included:

- Name
- Mailing address
- Phone number, mobile and/or home
- Email address
- Date of birth
- Social Security number
- 1099 Forms
- Driver’s license number, Passport number, or other state or government IDs (including photocopies of such)
- Vehicle information, such as Vehicle Identification Number or License Plate Number

0000001



- Tax documents, including Tax Returns and Tax Forms and individual taxpayer identification number
- Credit or Debit card numbers
- Bankruptcy filings
- Financial statements and financial account numbers plus a security code, access code, or password that may permit access the account
- Credit reports, including credit score and credit history
- Loan applications
- Medical information
- Digital signatures

What Are We Doing About It? Protecting the privacy and security of your personal information is of critical importance to Crossroads. Though we have no basis to believe that any of your personal information was misused, Crossroads is informing you of this incident because we respect your privacy.

On April 3, 2023, Crossroads secured access to its systems, began migrating all data to a cloud server with enhanced security, and implemented additional technical, and organizational controls.

On April 5, 2023, Crossroads notified the Federal Bureau of Investigation.

After conducting a full investigation of the incident, we have put in place additional security controls to protect against future attacks. This includes enhanced security around access to our system requiring a second form of user verification (MFA), more complex user-restricted access, redundant backup of the data, and continuous monitoring to protect against further incidents.

What Can You Do To Protect Yourself? You can protect yourself from identity theft by remaining vigilant and reviewing account statements and monitoring free credit reports from consumer reporting agencies.

To provide you with support as you monitor your personal information, Crossroads is offering two years of 1-bureau free credit monitoring through Experian. Please see the section below called “**How Do I Sign Up For Free Credit Monitoring?**” for more details about the services available to you and how to enroll.

Copy of Credit Report: For your convenience, we have provided contact information for the three nationwide credit reporting agencies below. These nationwide credit reporting agencies provide a free copy of your credit report, at your request, once every 12 months:

Equifax
 (800) 525-6285
 www.equifax.com
 Equifax Credit Information
 Services
 P.O. Box 740241
 Atlanta, GA 30374

Experian
 (888) 397-3742
 www.experian.com
 Experian National Consumer
 Assistance Center
 P.O. Box 4500
 Allen, TX 75013

TransUnion
 (800) 680-7289
 www.transunion.com
 TransUnion Consumer
 Relations
 P.O. Box 2000
 Chester, PA 19106-2000

You may also contact additional consumer reporting agencies by reviewing the list on the Consumer Financial Protection Bureau's website at <https://www.consumerfinance.gov/consumer-tools/credit-reports-and-scores/consumer-reporting-companies/companies-list/>.

Contact the Federal Trade Commission: The FTC provides further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580; by phone at 1-877-ID-THEFT (877-438-4338); or online at www.consumer.gov/idtheft.

Security Freeze: You have the ability to place a security freeze on your credit report at no charge. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent but may delay your ability to obtain credit. To place a security freeze, you must contact each of the three credit bureaus listed above and you may be required to provide your full name; Social Security number; date of birth; the addresses where you have lived over the past five years; proof of current address, such as a utility bill or telephone bill; a copy of a government issued identification card; and if you are the victim of identity theft, the police report, investigative report, or complaint to a law enforcement agency.

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 remove the security freeze, you must contact each of the three credit bureaus 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.

Place a Fraud Alert: At no charge, you can also have the three major credit bureaus place a fraud alert on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact the credit reporting agencies:

Equifax
(800) 525-6285
www.equifax.com
Equifax Credit Information
Services
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
Experian National Consumer
Assistance Center
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 680-7289
www.transunion.com
TransUnion Consumer
Relations
P.O. Box 2000
Chester, PA 19106-2000

Suspected Identity Theft: Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law

0000001



enforcement, your state attorney general, or the U.S. Federal Trade Commission (“FTC”). Residents of the District of Columbia, Maryland, New York, and North Carolina may contact their state attorneys general at the addresses below.

- **Office of the Attorney General for the District of Columbia**, 406 6th Street NW, Washington, D.C. 20001; 202-727-3400, <https://oag.dc.gov/>
- **Maryland Office of the Attorney General**, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; toll-free at 888-743-0023; <https://www.marylandattorneygeneral.gov/>
- **New York Office of the Attorney General** at: The Capitol, Albany, NY 12224-0341; <http://www.ag.ny.gov/home.html>; 800-771-7755; or **New York Department of State Division of Consumer Protection** at: One Commerce Plaza, 99 Washington Avenue, Albany, New York 12231-0001; <https://dos.ny.gov/consumer-protection>; 800-697-1220.
- **North Carolina Attorney General’s Office**, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-566-7226 (Toll-free within North Carolina) or 919-716-6000; www.ncdoj.gov

Federal Fair Credit Reporting Act Rights: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.

Notice to Tennessee Residents:

TENNESSEE CONSUMERS HAVE THE RIGHT TO OBTAIN A SECURITY FREEZE

You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze must be requested in writing by certified mail or by electronic means as provided by a consumer reporting agency. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. If you are actively seeking a new credit, loan, utility, or telephone account, you should understand that the procedures involved in lifting a security freeze may slow your applications for credit. You should plan ahead and lift a freeze in advance of actually applying for new credit. When you place a security freeze on your credit report, you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or authorize the release of your credit report for a period of time after the freeze is in place. To provide that authorization you must contact the consumer reporting agency and provide all of the following:

- (1) The personal identification number or password;
- (2) Proper identification to verify your identity; and
- (3) The proper information regarding the period of time for which the report shall be available.

A consumer reporting agency must authorize the release of your credit report no later than fifteen (15) minutes after receiving the above information. A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account, that requests information in your credit report for the purposes of fraud control, or reviewing or collecting the account. Reviewing the account includes activities related to account maintenance.

You should consider filing a complaint regarding your identity theft situation with the federal trade commission and the attorney general and reporter, either in writing or via their web sites.

How Do I Sign Up For Free Credit Monitoring?

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by May 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll:
<https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-1317 by May 31, 2024. Be prepared to provide engagement number B116897 as proof of eligibility for the Identity Restoration services by Experian.



ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* 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.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call 833-918-1317 toll-free Monday through Friday from 8 am – 8 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B116897.

You may also contact us by writing to: Crossroads Equipment Lease & Finance, LLC, c/o Chief Executive Officer, 9385 Haven Ave., Rancho Cucamonga, CA 91730.

Sincerely,



Crossroads Equipment Lease & Finance, LLC