



LEWIS BRISBOIS BISGAARD & SMITH LLP

Lauren D. Godfrey
One PPG Place, 28th Floor
Pittsburgh, Pennsylvania 15222
Lauren.Godfrey@lewisbrisbois.com
Direct: 412.567.5113

December 7, 2022

VIA WEBSITE PORTAL

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330
Email: breach.security@maine.gov

Re: Notification of Data Security Incident

Dear Attorney General Frey:

Lewis Brisbois represents Veros Credit, a provider of auto financing solutions located in Santa Ana, California, in conjunction with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maine's data breach notification law.

1. Nature of the Security Incident

On December 10, 2021, Veros Credit discovered suspicious activity in its digital environment consistent with a ransomware attack. Upon discovering this activity, Veros Credit immediately took steps to secure its digital environment and engaged leading cybersecurity experts to conduct an investigation to determine what happened and whether personal information may have been accessed or acquired in conjunction with the incident. The investigation revealed that an unknown actor gained access to and may have obtained data from the Veros Credit network without authorization. Veros Credit subsequently initiated a comprehensive review of the affected files through independent experts to determine whether they contained personal information belonging to individuals. After a thorough investigation, on November 22, 2022, Veros Credit identified the individuals who may have had sensitive personal information exposed during the incident.

2. Type of Information and Number of Maine Residents Affected

Veros Credit notified 3 residents of Maine of this data security incident via first class U.S. mail on December 5, 2022. The information accessed and potentially acquired by the unauthorized actor responsible for this incident may have included name and Social Security number, driver's license or state identification card number, financial account number, passport number, username and password, health insurance information,

and medical information. A sample copy of the notification letter sent to these individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

Veros Credit reported this incident to the Federal Bureau of Investigation and will cooperate with investigative efforts in an attempt to hold the perpetrator(s) of this incident responsible, if possible. Veros Credit has also implemented additional security features in an effort to prevent a similar incident from occurring in the future. Further, as referenced below Veros Credit has offered the individuals whose Social Security number, state identification card number, and/or passport number was involved 12 months of complimentary services through IDX, which includes credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

4. Contact Information

Veros Credit remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (421) 567-5113 or by email at Lauren.Godfrey@lewisbrisbois.com.

Regards,

Lauren D. Godfrey

Lauren D. Godfrey, CIPP/US, CIPP/E of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enc.: Sample Consumer Notification Letter



P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
(833) 896-6977
Or Visit:
<https://response.idx.us/veros>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

December 5, 2022

Re: Notice of Data <<Variable Text 1>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you about a data security incident that may have involved your personal information. We take the privacy and security of the personal information in our care very seriously and that is why we are notifying you about the incident, offering you credit monitoring and identity monitoring services, and informing you about steps you can take to help protect your personal information.

What Happened? On December 10, 2021, Veros Credit was alerted to a suspicious cybersecurity incident within its digital network. We immediately undertook an investigation to determine what happened. We hired experts to help determine whether sensitive personal information was at risk during the incident, what that information might be, and whose information might have been involved in the incident. On November 22, 2022 we identified the individuals who had sensitive personal information potentially exposed during the incident. We then worked to locate those people. While we have no reason to believe that anyone's information has been misused, out of an abundance of caution, we are writing to inform you of the incident and to provide you with access to complimentary credit monitoring and identity protection services.

What Information Was Involved? The information involved may have included your name and <<Variable Text 2>>.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We also implemented additional safeguards to further increase the security of our network systems to minimize the likelihood of a similar event occurring in the future. We are also providing you with information about steps you can take to help protect your personal information. In addition, we are offering you complimentary identity monitoring and recovery services for <<12/24>> months through IDX, an industry leading expert in data protection and identity restoration services.

What You Can Do: We encourage you to review the recommendations on the following page to help protect your information. We also encourage you to enroll in the IDX identity protection services being provided to you, at no cost. To enroll, please visit the IDX website at <https://response.idx.us/veros> and provide your enrollment code located at the top of this page. Additional information describing the IDX identity protection services, along with other recommendations to protect your personal information, is included with this letter. Please note you must enroll by March 5, 2023.

For More Information: If you have questions or need assistance, please contact (833) 896-6977 or go to <https://response.idx.us/veros> so that we can answer any questions that you may have regarding this incident or the complimentary services being offered to you. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time.

Please know that we regret any worry or inconvenience that this may cause you.

Sincerely,

Veros Credit

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.