Locke Lord LLP

20 Church Street
20th Floor
Hartford, CT 06103
Telephone: 860-525-5065
Fax: 860-955-1145
www.lockelord.com

March 29, 2023

By Email

Attorney General John Formella
Office of the Attorney General
NH Department of Justice
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Re: Notice, RSA § 359-C:20.

To the Office of the Attorney General:

Our client Fora Financial LLC ("Fora Financial") provides commercial financing to small businesses. On behalf of Fora Financial, we hereby provide notice pursuant to RSA § 359-C:20 of a breach of security that may have affected the personal information of 11 residents of New Hampshire.

What Happened

On or about September 9, 2022, Fora Financial learned that one or more unauthorized third parties had obtained deal-related information that had been submitted to Fora Financial. Fora Financial immediately began to investigate, to determine whether (i) the information originated with Fora Financial, (ii) any leak or cybersecurity vulnerability may have been exploited to obtain the information, and (iii) any information obtained from Fora Financial without authorization included personal information of potentially affected individuals. Initially, Fora Financial believed the leak was limited to confidential business lead information and did not include personal information. Through its ongoing investigation, Fora Financial discovered that lead information it was able to acquire from third-parties matched information in Fora Financial's information system and included personal information. Fora Financial's forensics team determined that the source of the information was an exploit in its information systems, which was uncovered after an exhaustive investigation and terminated on February 19, 2023. On February 27, 2023, Fora's investigation determined that New Hampshire residents were among the population of individuals whose personal information was affected.

While Fora Financial has terminated the source of the compromise, its investigation is on-going. The apparent use by unauthorized persons of Fora Financial's deal information, including personal information, is apparently for competitive business purposes, and not to commit identity

theft or fraud. Therefore, Fora Financial does not believe affected individuals are at risk of identity theft or fraud as a result of this unauthorized use.

What Information Was Involved

This incident involved personal information,
. Other information included information concerning affected individuals' businesses that was submitted to Fora Financial in connection with potential transactions, including the businesses' financial information. We have no indication that the personal information of affected individuals has been used for any purpose other than to attempt to provide financial products to businesses.

What Fora is Doing

Once Fora Financial learned that one or more unauthorized persons had acquired Fora Financial's confidential deal information, Fora Financial took immediate steps to identify the source of the information, and any vulnerabilities in its systems and business processes that could have resulted in the unauthorized acquisition of the data. While Fora Financial has terminated the source of the compromise, its investigation is currently ongoing. Fora Financial is working to identify and notify affected individuals at this time in order provide them with information about what happened and to inform them of the steps they may take to protect themselves further. Fora Financial is providing credit monitoring and guidance on protections against identify theft to affected individuals. Notably, based on the specific activities of the threat actors and competitive business use of the information, Fora Financial does not believe this incident has resulted in a significant risk of identity theft or fraud to affected individuals.

Although Fora Financial does not believe that this incident has resulted in a significant risk of identity theft or fraud, Fora Financial, as previously stated, is offering credit monitoring services for one year at no cost to the affected individuals, including the 11 New Hampshire residents.

As required by RSA § 359-C:20, Fora Financial is providing notice of this incident to the affected individuals including the 11 New Hampshire residents by mail on or about March 29, 2023. A template for that notification letter is attached. On Fora Financial's behalf, we are providing notice of this incident to agencies in other states where affected individuals reside.

* * * * *

Please do not hesitate to contact me with any questions related to this matter.

Sincerely,

Theodore P. Augustinos

Attachments

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Fora Financial LLC ("Fora Financial") is contacting you about a security incident affecting your personal information. Fora Financial believes that certain deal related information you have provided to Fora Financial as part of a commercial financing application has been obtained without authorization by one or more Fora Financial's competitors who may seek to offer competing financial products. This information included certain of your personal information. As a result, Fora Financial is notifying you of this incident and offering to provide you credit monitoring services.

What happened?

On or about September 9, 2022, Fora Financial learned that one or more unauthorized third parties had obtained deal-related information that had been submitted to Fora Financial. Fora Financial immediately began to investigate, to determine whether (i) the information originated with Fora Financial, (ii) any leak or cybersecurity vulnerability may have been exploited to obtain the information, and (iii) any information obtained from Fora Financial without authorization included personal information of potentially affected individuals. Initially, Fora Financial believed the leak was limited to confidential business lead information and did not include personal information. Through its ongoing investigation, Fora Financial discovered that lead information it was able to acquire from third-parties matched information in Fora Financial's information system and included personal information. Fora Financial's forensics team determined that the source of the information was an exploit in its information systems, which was uncovered after an exhaustive investigation and terminated on February 19, 2023.

While Fora Financial has terminated the source of the compromise, its investigation is on-going. The apparent use by unauthorized persons of Fora Financial's deal information, including personal information, is apparently for competitive business purposes, and not to commit identity theft or fraud. Therefore, Fora Financial does not believe you are at risk of identity theft or fraud as a result of this unauthorized use.

What information was involved?

Your personal information included . Other information included information concerning your business that was submitted to us in connection with a potential transaction, including your business's financial information. We have no indication that your information has been used for any purpose other than to attempt to provide financial products to your business, but we wanted to make you aware of the incident, our efforts to safeguard your personal information, and resources you may use to protect yourself.

What we are doing.

Once we learned that one or more unauthorized persons had acquired Fora Financial's confidential deal information, we took immediate steps to identify the source of the information, and any vulnerabilities in our systems and business processes that could have resulted in the unauthorized acquisition of our data. While Fora Financial has terminated the source of the compromise, its investigation is currently ongoing. Fora Financial is providing identity monitoring and best practices on ways to minimize your chances of becoming a victim of identity theft for twelve months. Notably, based on the specific activities of the threat actors and competitive business use of the information, Fora Financial does not believe this incident has resulted in a significant risk of identity theft or fraud to you.

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
*You have until **<<b2b_text_6(activation deadline)>>** to activate your identity monitoring services.*
Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What you can do.
Although we do not believe there is a risk of identity theft or fraud to you following this event, we recommend that you remain vigilant and review your account statements and credit reports regularly, and report any concerning transactions to your financial services provider. Please review the instructions attached to this letter to access your complementary credit monitoring services provided by Fora Financial.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.
If you have questions, please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

John Viskocil
General Counsel, Chief Compliance Officer

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft and you will not be charged a fee to obtain a security freeze.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You can also contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 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 D.C.: You have the right to place a fraud alert or security freeze. For more information on how to place a fraud alert or security freeze, you can contact the Federal Trade Commission or any of the consumer reporting bureaus as described above. You can also contact the D.C. Attorney General at (202) 442-9828 or consumer.protection@dc.gov.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.