Lindsay B. Nickle, Partner & Vice Chair
Cybersecurity & Data Privacy Team
1201 Elm Street, Suite 2550
Dallas, Texas 75270

April 2, 2024

VIA ELECTRONIC MAIL
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03302
E-Mail: doj-cpb@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP represents On Q Financial, LLC ("On Q Financial"), in connection 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 New Hampshire's data breach notification statute.

Nature of the Security Incident

On February 20, 2024, On Q Financial received a notification from ConnectWise, a software and IT management provider, regarding a vulnerability involving its product, ScreenConnect, which is a software program On Q Financial used for remote access to computers in our network. In response to the notification received from ConnectWise, On Q Financial immediately patched and upgraded the application and began an investigation. The investigation revealed some suspicious activity through the Screen Connect application. On Q Financial engaged a computer forensics investigation firm to conduct an independent investigation into what happened and determine whether personal information may have been accessed or acquired without authorization. Our investigation confirmed that the ConnectWise vulnerability has been successfully patched and the On Q Financial computer network is secure. However, on March 14, 2024, the investigation determined that the ConnectWise vulnerability permitted an unknown individual to gain access to our computer network and the personal information of some of our clients was exfiltrated from our network. The information affected may have included .

Number of New Hampshire Residents Involved

On March 29, 2024, On Q Financial notified eighty-seven (87) New Hampshire residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

Steps Taken to Address the Incident

In response to the incident, On Q Financial is providing individuals with information about steps they can take to help protect their personal information. Additionally, On Q Financial is offering individuals complimentary identity protection services. These services include of credit monitoring and proactive fraud assistance to help with any questions that individuals might have or if an individual becomes a victim of fraud. Also, after receiving notification from ConnectWise, On Q Financial immediately patched and upgraded the application and has confirmed that there is no persistence in the environment. On Q Financial has also reported the incident to the Federal Bureau of Investigation and will cooperate with any resulting investigation.

Contact Information

On Q Financial remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at

Sincerely,

Lindsay B. Nickle
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter

On Q Financial, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

March 29, 2024

Re: Notice of Data Security Incident

Dear [redacted]:

On Q Financial LLC ("On Q Financial") is writing to notify you about a data security incident that may have involved your personal information. On Q Financial takes the privacy and security of all information in its possession very seriously. Please read this letter carefully, as it contains information regarding the incident and information about steps that you can take to help protect your information.

What Happened? On February 20, 2024, On Q Financial received a notification from ConnectWise, a software and IT management provider, regarding a vulnerability involving its product, ScreenConnect, which is a software program On Q Financial used for remote access to computers in our network. In response to the notification received from ConnectWise, we immediately patched and upgraded the application and began an investigation. The investigation revealed some suspicious activity through the Screen Connect application. On Q Financial engaged a computer forensics investigation firm to conduct an independent investigation into what happened and determine whether personal information may have been accessed or acquired without authorization. Our investigation confirmed that the ConnectWise vulnerability has been successfully patched and the On Q Financial computer network is secure. However, on March 14, 2023, the investigation determined that the ConnectWise vulnerability permitted an unknown individual to gain access to our computer network and the personal information of some of our clients was exfiltrated from our network. Please note that at this time we are not aware of any evidence that any of our clients' personal information has been misused, and out of an abundance of caution, we are notifying all of our clients whose personal information has potentially been impacted.

What Information was Involved? The information that may have been affected in connection with this incident includes your .

What Are We Doing? As soon as ConnectWise notified us about the vulnerability, we installed the patch and began the investigation discussed above. We have also reported this incident to the FBI and will cooperate in any resulting investigation. To reduce the likelihood of a similar incident occurring in the future, we have also implemented additional measures to enhance the security of our network environment.

In addition, while we have no evidence that any of your personal information has been misused, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for from the date of enrollment when changes occur to your credit file. This notification will be sent to you on the same day that the change or update occurs with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do. We recommend that you review the guidance included with this letter about how to protect your personal information. In addition, please enroll in the complimentary credit monitoring services, please log on to **https://secure.identityforce.com/benefit/onqfinancial** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

To receive the monitoring services described above, you must enroll within 90 days from the date of this letter. Enrollment requires an internet connection and e-mail account and may not be available to minors under 18[1]. Please note that when signing up for monitoring services, you may be asked to verify your family member's personal information to confirm your family member's identity.

For More Information: Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call 1-833-961-6142 Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding major U.S. holidays. TransUnion representatives are fully versed on this incident and can answer any questions or concerns you may have.

We take your trust in On Q and this matter very seriously. Please accept our apologies for any concern or inconvenience this may cause you.

Sincerely,

R. Patrick Lamb
Chief Executive Officer

1. To receive credit monitoring 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.

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
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 to know 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://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.