



Laura K. Funk, Partner
Cybersecurity & Data Privacy Team
1201 Elm Street, Suite 2550
Dallas, Texas 75270
LFunk@constangy.com
Mobile: 248.709.9385

April 21, 2023

VIA ELECTRONIC SUBMISSION

Attorney General Brian Frosh
Maryland Attorney General's Office
Consumer Protection Division
200 St. Paul Place
Baltimore, Maryland 21202
Email: idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh,

Constangy, Brooks, Smith & Prophete, LLP ("Constangy") represents Quo Vadis Financial Management Inc. ("Quo Vadis") in connection with the data security incident described below.

Nature of the Security Incident.

On September 26, 2022, Quo Vadis discovered suspicious activity associated with one of its email accounts. In response, Quo Vadis took immediate steps to secure its email environment and promptly launched an investigation. In so doing, Quo Vadis engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been impacted. On October 13, 2022, Quo Vadis received confirmation that one email account was accessed without authorization and then engaged a vendor to review the potentially impacted items likely to contain personal information. As a result, on January 13, 2023, Quo Vadis learned that personal information belonging to certain individuals associated therewith may have been impacted. Quo Vadis then took steps to verify the identity of those individuals and identify current mailing addresses to effectuate notification. The address collection process was completed on February 7, 2023, after which Quo Vadis arranged to provide notification of the incident.

The information that may have been accessible by the malicious actor(s) responsible for this incident includes Social Security numbers.

Number of Maryland Residents Affected.

Quo Vadis notified 6 Maryland residents of this incident via First-Class US Mail on February 24, 2023. A sample copy of the notification letter is included with this correspondence. A total of 569 individuals from varying jurisdictions were notified.

Steps Taken Relating to the Incident.

As soon as Quo Vadis discovered this incident, Quo Vadis implemented measures to enhance the security of its email environment in an effort to minimize the risk of a similar incident occurring in the future.

Quo Vadis has established a toll-free call center through IDX, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available at 1-800-939-4170 from 8:00 A.M. to 8:00 P.M. Central Time, Monday through Friday (excluding holidays). In addition, while Quo Vadis is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Quo Vadis is also providing complimentary credit monitoring and identity protection services to notified individuals.

Contact Information.

Quo Vadis remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me directly at lfunk@constangy.com.

Best regards,

A handwritten signature in black ink, appearing to read 'L. Funk', with a long, sweeping horizontal line extending to the right.

Laura K. Funk
Constangy, Brooks, Smith & Prophete LLP

Enclosure: Sample Notification Letter

Quo Vadis Financial
10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223



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

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXX>>

February 24, 2023

Subject: Notice of Data <<Variable Text 1: Breach or Security Incident>>

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

I am writing to inform you of a data security incident experienced by Quo Vadis Financial Management, LLC (“Quo Vadis”) that may have affected your personal information. We take the privacy and security of all information within our possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

What Happened. On September 26, 2022, Quo Vadis discovered suspicious activity associated with one of our email accounts. In response, we took immediate steps to secure our email environment and promptly launched an investigation. In so doing, Quo Vadis engaged independent digital forensics and incident response experts to determine what happened and to identify any personal information that may have been impacted. On October 13, 2022, we received confirmation that one employee email account was accessed without authorization. We then engaged a vendor to review the mailbox to identify impacted items likely to contain personal information. As a result, on January 13, 2023, Quo Vadis learned that certain personal information may have been accessed or acquired without authorization. Following a thorough review of all personal information contained in the mailbox, identification of all potentially impacted individuals, and verification of current mailing addresses for the individuals, it was confirmed on February 7, 2023, that your information may have been accessed or acquired as a result of the incident.

Notably, we have no evidence of the misuse or attempted misuse of any potentially impacted personal information.

What Information Was Involved. The information potentially impacted in connection with this incident included your name as well as your <<insert data sets>>.

What Are We Doing. As soon as Quo Vadis discovered this incident, we took the steps described above. In addition, Quo Vadis implemented measures to enhance the security of its email environment in an effort to minimize the risk of a similar incident occurring in the future.

Although we have no evidence of the misuse of any potentially impacted personal information, we are providing you with information about steps that you can take to help protect your personal information and offering you complimentary identity protection services through IDX – a data breach and recovery services expert. These services include <<12 / 24 months>> of credit and dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help to resolve issues if your identity is compromised.

The deadline to enroll in these services is May 24, 2023. 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.

What You Can Do: You can follow the recommendations on the following page to help protect your information. We also encourage you to enroll in the complimentary services being offered to you through IDX by using the enrollment code provided above.

For More Information: Further information about how to protect your information appears on the following page. If you have questions or need assistance, please call IDX at 1-800-939-4170 from 6:00 A.M. to 6:00 P.M. Pacific Time, Monday through Friday (excluding holidays). IDX call center representatives are fully versed on this incident and can answer any questions that you may have.

Please accept my sincere apologies and know that we take this matter very seriously and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in dark ink, appearing to read "Andrew R. Pike". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Andrew Pike, CEO
Quo Vadis Financial Management LLC
1160 Aikoo Place
Pearl City, Hawaii 96782

STEPS YOU CAN TAKE TO HELP PROTECT YOUR 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 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
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, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

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

441 4th 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://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.