



February 21, 2023

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

RECEIVED

FEB 24 2023

CONSUMER PROTECTION

Dear Attorney General Formella:

Second Alpha Partners is notifying you, pursuant to NH Rev. Stat. § 359-C:20, of cybersecurity events involving an email account used by a Second Alpha Partners employee. Second Alpha Partners is a private equity firm headquartered in New York, New York.

We have learned that an unauthorized third party or parties may have gained access to a single email account used by a Second Alpha Partners employee, which contained certain personal information of some of our investors. Based on our investigation into this incident to date, we believe that this unauthorized activity began on or prior to October 12, 2022, and ended not later than November 25, 2022. The incident was discovered by Second Alpha Partners on November 24, 2022. We promptly took steps to secure the email account by resetting the email account password (which was completed on November 25, 2022), and initiated an investigation with the assistance of a third party forensic firm.

We have also learned of a successful phishing attempt on December 20, 2022, that resulted in an unauthorized third party or parties gaining access to the same Second Alpha Partners' email account. We promptly took steps to secure the email account by resetting the email account password on December 20, 2022. In the course of our investigation, on January 23, 2023, we determined that personal information may have been accessed during these incidents.

Our investigation has not determined whether these incidents are connected or caused by the same unauthorized third party or parties. We have not identified any evidence that the third party or parties downloaded any content from the email account.

To date, we have determined that the
of one (1) New Hampshire resident may have been accessed by an unauthorized third party. Our investigation remains ongoing.

We are offering this individual eighteen months of complimentary identity theft and credit monitoring services through Kroll. We also provided the individual with our contact information so we can respond to individual's questions.

Attached is an anonymized version of the notification letter we sent to the New Hampshire resident on February 21, 2023.

We take this matter very seriously and are committed to answering any questions you may have regarding this incident or this submission.

Sincerely,

Eugene Galantini
Second Alpha Partners
276 Fifth Avenue, Suite 204
New York, NY 10001



<<Name>>
<<Address>>
<<Address>>

February 21, 2023

NOTICE OF SECURITY INCIDENT

Dear <<Name>>,

We are writing to let you know about cybersecurity incidents that affected the email account of an individual at Second Alpha Partners that contained the personal information of some Second Alpha Partners' investors, including your personal information. We are providing this notice to outline some steps you can take to help protect yourself.

Keeping personal information safe and secure is very important to Second Alpha Partners, and we continue to prioritize to protecting that information. We sincerely regret any inconvenience this matter may cause you.

WHAT HAPPENED?

We have learned that an unauthorized third party or parties may have gained access to a single email account used by a Second Alpha Partners employee, which contained certain personal information of some of our investors. Based on our investigation into this incident to date, we believe that this unauthorized activity began on or prior to October 12, 2022, and ended not later than November 25, 2022. The incident was discovered by Second Alpha Partners on November 24, 2022. We promptly took steps to secure the email account by resetting the email account password (which was completed on November 25, 2022), and initiated an investigation with the assistance of a third party forensic firm.

We have also identified a successful phishing attempt on December 20, 2022, that resulted in an unauthorized third party or parties gaining access to the same Second Alpha Partners' email account. We promptly took steps to secure the email account by resetting the email account password on December 20, 2022. Our investigation has not determined whether these incidents are connected or caused by the same unauthorized third party or parties.

WHAT INFORMATION WAS INVOLVED?

The personal information that may have been exposed may include your

We have no information suggesting that any of your personal information has been misused.

WHAT WE ARE DOING

Upon learning about this unauthorized activity, we promptly began an investigation by engaging a third party forensic investigator, and took action to remove the unauthorized access to the affected email account.

We have also secured the services of Kroll to provide identity monitoring services at no cost to you for eighteen months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

February 21, 2023

Activation Code: <<Activation Code>>

Verification ID: <<Verification ID>>

Below please find information to register for a complimentary membership to Kroll's identity monitoring services.

The identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit [Enroll.krollmonitoring.com/redeem](https://enroll.krollmonitoring.com/redeem) to activate and take advantage of your identity monitoring services.

You have until May 18, 2023 to activate your identity monitoring services.

Activation Code: <<Activation Code>>

Verification ID: <<Verification ID>>

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

Additional information describing your services is included at the end of this letter.

WHAT YOU CAN DO

We encourage you to contact Kroll and take advantage of the identity monitoring services that we are providing to you free of charge. In addition, you should remain vigilant and carefully review your accounts and credit reports for any suspicious activity. This is a best practice for all consumers.

As noted above, we have no evidence that your information has been misused. However, as always, if you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or other company with which the account is maintained and any relevant government agency.

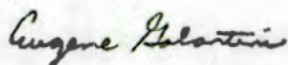
If you would like to take additional steps to help protect your personal information, attached to this letter are helpful resources on how to do so, including recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

FOR MORE INFORMATION

We take our responsibility to protect your information very seriously, and we sincerely regret any inconvenience that this matter may cause you.

If you have any questions, please contact us at _____, Monday through Friday from 9:00 a.m. to 5:00 p.m. Eastern Time, excluding major U.S. holidays. Please have your Activation Code and Verification ID ready.

Sincerely,



Eugene Galantini
Second Alpha Partners
276 Fifth Avenue, Suite 204
New York, NY 10001

Additional Resources

Below are additional helpful tips you may want to consider to help protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. 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 law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

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 <https://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at <https://www.annualcreditreport.com/manualRequestForm.action>. Credit reporting agency contact details are provided below.

Equifax:

equifax.com
equifax.com/personal/credit-report-services
P.O. Box 740241
Atlanta, GA 30374
866-349-5191

Experian:

experian.com
experian.com/help
P.O. Box 2002
Allen, TX 75013
888-397-3742

TransUnion:

transunion.com
transunion.com/credit-help
P.O. Box 1000
Chester, PA 19016
888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 1 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. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. 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 credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. 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 telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado, Delaware, and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

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

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, <http://www.marylandattorneygeneral.gov>, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, <http://www.ncdoj.gov>, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

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

For Georgia, Maryland, New Jersey, 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 bureaus directly to obtain such additional report(s).



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will 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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.