Wyrick Robbins Yates & Ponton LLP
ATTORNEYS AT LAW
4101 Lake Boone Trail, Suite 300, Raleigh, NC 27607
PO Drawer 17803, Raleigh, NC 27619
P: 919.781.4000 F: 919.781.4865 www.wyrick.com
MEMBER OF MERITAS LAW FIRMS WORLDWIDE

ALEX M. PEARCE, ESQ.
Apearce@wyrick.com

April 21, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

I am writing to notify you that our client, Rialto Markets LLC ("Rialto"), experienced a data incident involving Maryland residents.

Rialto is a broker-dealer that offers a platform for investors to take advantage of investment offerings, including the offerings of issuer clients for whom Rialto provides certain administrative services. Rialto became aware of suspicious activity in one of its employees' email accounts on February 24, 2022. The company immediately took steps to secure the email account and promptly began an investigation with the assistance of outside cybersecurity and forensic experts to determine what had occurred. Through that investigation, Rialto determined that an unauthorized third party had access to the employee's email account between November 30, 2021, and February 25, 2022. The unauthorized access was limited to one email account, and the company has no evidence to indicate that the incident affected any of its other information systems.

As part of its investigation, on March 29, 2022, Rialto discovered that the affected email account contained files that included personal information of Maryland residents. Rialto currently believes the incident affected the personal information of approximately. The company's investigation revealed that the information affected may have included one or more of the following data elements: date of birth, Social Security Number, driver's license or other government-issued identification number, financial account information including routing number or institution name, credit or debit card information including number, security code or PIN, or expiration date, IRS PIN number, access credentials for online accounts, or email address plus security question and answer that could permit access to an online account. At this time, Rialto's investigation cannot conclusively determine whether the unauthorized party actually viewed any of these files. Nevertheless, Rialto is notifying 84 affected Maryland residents by U.S. Mail on April 21, 2022. A sample copy of the individual notification letter is enclosed.

Rialto is offering the affected individuals two years of complimentary credit monitoring and other consumer protection services, including fraud loss reimbursement insurance coverage. Also in response to the incident, Rialto implemented additional access controls and enhanced system logging for its corporate email system. The company is continuing to evaluate additional controls.

Thank you for your time and attention to this matter. Please let us know if you have any questions or concerns regarding this notice or the incident.

Very truly yours,

WYRICK ROBBINS YATES & PONTON LLP

Alex M. Pearce

Enclosure

Rialto markets

<<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>>,

We are writing to tell you about a data security incident that affected our email system. Some of your personal information was included in our email system, so we want to let you know what occurred, what we are doing to address it, and how you can activate the identity monitoring services we are offering.

What happened?
As you may know, Rialto Markets LLC is a broker-dealer that offers a platform for investors to take advantage of investment offerings. We also provide certain services to issuer clients with whom you may have a relationship. On February 24, 2022, we became aware of some suspicious activity in one of our employees' email accounts. We immediately took steps to secure the email account and promptly began an investigation with the assistance of outside cybersecurity and forensic experts to determine what had occurred. That investigation determined that an unauthorized third party had access to the employee's email account between November 30, 2021, and February 25, 2022. The unauthorized access was limited to one email account, and we have no evidence to indicate that the incident affected any of our other information systems. On March 29, 2022, we discovered that the affected email account contained files that included some of your personal information.

What information was involved?
Our investigation has determined that the affected email account contained files that included your <<b2b_text_1 (Impacted Data)>>. Although our investigation cannot conclusively determine whether the unauthorized party actually viewed any of this personal information, and we have no evidence that any information about you has been misused, we value your trust and believe it is important to notify you of this incident so that you can take steps to help protect yourself.

What we are doing.
As described above, when we discovered the unauthorized access, we took steps to secure the account and promptly began an investigation to determine what had occurred. In addition, we have implemented additional access controls and enhanced system logging for our corporate email system, and we continue to evaluate additional controls.

To help relieve concerns and restore confidence following this incident, we have also secured the services of Kroll to provide identity monitoring at no cost to you for two years. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. These services are described in more detail in the "Additional Resources" section included with this letter.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until ***<<b2b_text_6 (Date)>>*** *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.

What you can do.
Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, such as remaining vigilant by regularly reviewing your account statements and monitoring credit reports. This enclosure also provides contact details for the Federal Trade Commission and credit reporting agencies as well as information on how to place fraud alerts and security freezes.

For more information.
If you have questions, please call (855) 482-1556, 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.

We regret this incident and apologize for any inconvenience. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Shari Noonan
Chief Executive 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. Pursuant to 15 U.S.C. § 1681c-1, 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 Washington, D.C. residents: You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, www.oag.dc.gov, 1-202-727-3400.

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.

For Rhode Island residents: You may contact the Rhode Island Attorney General, 150 South Main Street, Providence, Rhode Island, 02903, 1-401-274-4400, www.riag.ri.gov.

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.

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: To file a police report or request any police reports that are available, contact law enforcement.

Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, D.C. 20552.

- 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.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty personnel have additional rights.

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.

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.