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

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

<<b2b_text_2 (NOTICE OF DATA [SECURITY INCIDENT / BREACH])>>

Dear <<first_name>> <<last_name>>,

Regal Securities is writing to let you know about a data security incident that may have affected a limited amount of your personal information. We are a securities brokerage firm and we may have received your personal information to provide you with financial services. We take the privacy and security of your information seriously and we would like to furnish you with the necessary information and actions we have taken to address this matter. This letter contains information about what occurred, steps you can take to protect your information, and resources we are making available to help you.

First and foremost, after a thorough investigation, we want to assure you that there is no evidence to suggest that your personal information has been used in an unauthorized manner.

What happened?
In February 2023, we discovered suspicious activity that impacted our ability to access some of our systems. We immediately implemented our incident response protocols, disconnected affected systems, and engaged external cybersecurity experts to conduct a forensic investigation. This investigation found that some information stored on our systems may have been compromised. Out of an abundance of caution, a vendor was hired to do an in-depth review of the potentially impacted data to determine if any personal information may have been present. This comprehensive review was completed in July 2023, at which point we identified that some of your personal information may have been affected. While we have no evidence that your personal information was misused, we wanted to notify you about this incident and provide you with resources to protect yourself.

What information was impacted?
From the review, it appears that your name and some combination of the following data elements may have been impacted by this incident: <<b2b_text_1 (data elements)>>.

What we are doing:
Cyber incidents are constantly evolving and we want to assure you we have taken significant steps to prevent such events. We have conducted a comprehensive review of our systems, strengthened our network defenses and our dedicated IT team has implemented additional security and ongoing monitoring to further safeguard your information.

For your peace of mind, we have secured the services of Kroll to provide identity monitoring services at no cost to you for two (2) years. 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. 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. To activate these services, please visit the link in this next paragraph:

What you can do:

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

You have until <<b2b_text_6 (activation 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.

Additional information describing your identity monitoring services is included on the next page.

It is always a good idea to remain vigilant for evidence of identity theft or fraud, to review your bank account and other financial statements as well as your credit reports for suspicious activity, and promptly report any suspicious activity to your financial institution. 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 any questions or concerns, please call **(866) 676-4046,** Monday through Friday, from 8:00 am to 5:30 pm Central Time, excluding major U.S. holidays. Protecting your information and maintaining your confidence while continuing to provide you with services to help you meet your financial goals remain our top priorities.

Sincerely,

Regal Securities

Regal Securities

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.

ADDITIONAL RESOURCES

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in Kroll's identity protection, notify them immediately by calling or by logging into Kroll's website and filing a request for help.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

4. You can obtain additional information about the steps you can take to avoid identity theft from the Federal Trade Commission. The FTC also encourages those who discover that their information has been misused to file a complaint with them. Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.