December 22, 2022

VIA EMAIL
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Security Incident Notification

To Whom It May Concern:

Apex Clearing Corporation ("Apex") is notifying your office with respect to a data security event involving certain personal information of New Hampshire residents. By providing this notice, Apex does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Apex is a broker-dealer, registered with the SEC and is a FINRA member. Apex provides brokerage services to Vimvest Securities, LLC d/b/a Monorail Securities ("Monorail"), which is an SEC registered investment advisor, to enable Monorail's customers to open brokerage accounts and trade U.S. securities through Monorail's application. This notice is solely regarding potential impact to personal information that may have occurred on Apex's systems.

Nature of the Security Incident

In late August and early September, Apex learned from Monorail that an unauthorized individual had used system credentials that Apex issued to Monorail to access Apex's systems and apparently defrauded some number of individual customers of Monorail. These fraudulent withdrawals were either recovered or reimbursed by Monorail. Apex immediately reset Monorail's credentials, began an investigation, and implemented additional safeguards to protect Apex's systems.

In late October, Monorail subsequently informed Apex that Monorail's new credentials were again used by an unauthorized person. These additional fraud attempts were blocked or recovered. Apex's analysis revealed that an unauthorized individual may have had access to Apex's systems between March 2022 and October 2022 as a result of the foregoing credential compromises.

On or after December 1, 2022, Apex discovered that certain personal information of New Hampshire residents may have been exposed. This personal information may have included the following types of personal information: first and last name; last four digits of Social Security

Number; Apex internal financial account number; address and contact information; bank account no.; and routing no.

Steps Taken in Response to the Security Incident

As part of the investigation, a leading forensic investigator was engaged to help determine the extent of access and exposure. Apex has also taken steps, including as described above, to enhance its data security measures to prevent the occurrence of a similar event.

Apex is sending notification letters to the affected New Hampshire residents on December 22, 2022 via regular U.S. mail. A copy of the template notification letter is enclosed. In addition, Apex is offering complimentary credit monitoring and identity protection services through Kroll to certain affected individuals for 12 months.

Apex has made a report to FINRA about these events. Apex has also notified law enforcement.

Number of New Hampshire Residents Impacted

Apex has identified 18 New Hampshire residents who were potentially impacted by this incident.

Contact Information

McDermott Will and Emery is our legal counsel in this matter. Accordingly, please direct all correspondence and questions to our counsel, Mark Schreiber, at mschreiber@mwe.com**,** (617)-535-3982, or by mail at 200 Clarendon Street, Floor 58, Boston, MA 02116-5021.

Sincerely,

Rajeev Khurana

Chief Legal Officer

Apex Clearing Corporation

Enc.

Template Notification Letter

<<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 sending you this notice because of a recent data security incident that occurred at Apex Clearing Corporation ("Apex") that may have involved your personal information. Apex received your information as a result of its relationship with Vimvest Securities, LLC d/b/a Monorail Securities ("Monorail"). Apex provides you with brokerage services through Monorail.

WHAT HAPPENED?

An unauthorized person gained access to Monorail's credentials to the Apex systems and subsequently used Monorail's credentials to access accounts on Apex systems. This unauthorized access to Apex systems occurred between March 2022 and October 2022.

Upon learning of this incident, Apex provided new credentials to Monorail and implemented additional precautions designed to further prevent unauthorized access to Apex systems. Apex promptly launched an investigation and a leading cybersecurity forensics firm was engaged to assist in the investigation. We subsequently notified law enforcement.

We recently discovered that certain personal information from your account or your application for an account with Apex may have been exposed. As a result, we are notifying you of certain steps we are taking to help protect your personal information.

WHAT INFORMATION WAS INVOLVED?

The information that the unauthorized individuals may have accessed includes: <<b2b_text_1(data elements)>>.

WHAT WE ARE DOING

Apex takes the protection of your personal information very seriously, and we are committed to protecting it. As an added precaution, Apex would like to offer you 12 months of identity monitoring services from Kroll at no cost to you. 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, Fraud Consultation, and Identity Theft Restoration.

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

You have until <<b2b_text_6(activation deadline)>> 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 services is included with this letter.

WHAT YOU CAN DO

In addition to activating the identity monitoring services we have arranged on your behalf, we recommend that you review your personal account statements, including your Monorail account statements (if you have a Monorail account), and credit reports to detect errors resulting from the security breach and immediately report any suspicious activity. Because you may become a victim of fraud, we also encourage you to review the "Steps You Can Take To Further Protect Your Information" sheet enclosed with this letter, which contains important information on placing fraud alerts and other important topics. You should always remain vigilant for the next 12 to 24 months for threats of fraud and identity theft by regularly reviewing your account statements and credit reports for errors or fraud. We recommend that you periodically obtain credit reports from each nationwide credit reporting agency and have information related to fraudulent transactions deleted.

MORE INFORMATION

We apologize for any inconvenience that this incident may cause you. If you have any questions or concerns, please contact (855) 624-2912, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some major U.S. holidays, or contact us by mail at 350 North St. Paul Street, Suite 1300, Dallas, TX 75201.

Sincerely,

Apex Clearing Corporation

STEPS YOU CAN TAKE TO FURTHER 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 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, including:

Equifax	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-916-8800
www.equifax.com	www.experian.com	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 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

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/articles/pdf-0096-fair-credit-reporting-act.pdf.

If you are a Connecticut resident, you may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

If you are a District of Columbia resident, you may contact the District of Columbia Office of the Attorney General to obtain information about steps to take to avoid identity theft at: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001 or by phone at 202-727-3400 or you may may visit https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft.

If you are an Iowa resident, state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

If you are a Maryland resident, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, or by sending an email to idtheft@oag.state.md.us, calling 410-576-6491, or writing to Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202.

If you are a New Mexico resident, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

If you are a New York resident, 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/.

If you are a North Carolina resident, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226 (Toll-free within North Carolina) 919-716-6000.

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and to the FTC.

If you are a Rhode Island resident, you can request additional information by contacting the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov/, (401) 576-6491. If you are, or suspect you are, a victim of identity theft, you may also obtain or file a police report by contacting your local police department to file a report. The report may be filed in the location in which the offense occurred, or the city or county in which you reside. When you file the report, provide as much documentation as possible, including copies of debt collection letters, credit reports, and your notarized ID Theft Affidavit.

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.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help 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.