



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

March 1, 2022

Bruce A. Radke
312.463.6211
312.873.3763 Fax
bradke@polsinelli.com

Via Electronic Mail – Idtheft@oag.state.md.us

Office of the Attorney General
Attn: Jeff Karberg, Administrator of the Identity Theft Program
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Breach

Dear Mr. Karberg,

We are writing to your office on behalf of our Client, Cornelius, Stegent, and Price LLP, and its affiliate, Stegent Equity Advisors, Inc. (hereafter, “CSP” or “Client”). On or about September 29, 2021, Client discovered that an unknown individual accessed a business email account without authorization. Client immediately began measures to limit access to sensitive personal information and retained the services of a specialized cybersecurity firm to help investigate the Incident.

The investigation determined that, while there was no evidence that the unauthorized individual attempted to view or improperly use any of individuals’ information, as a result of the Incident, the unauthorized individual would have had access to copy the mailbox data. CSP immediately reported the Incident to TD Ameritrade and our other key business partners to mitigate the risk of any fraudulent activity.

There was no evidence to suggest that the unauthorized individual compromised any other of CSP’s other email accounts or systems. However, in an abundance of caution, CSP retained an eDiscovery vendor to analyze the mailbox and determine whether any sensitive financial information was impacted. On or about January 7, 2022, the eDiscovery vendor confirmed that the account contained some sensitive personal information.

CSP has not discovered any specific evidence of fraud or identity theft. However, in an abundance of caution, CSP will be providing credit monitoring services to potentially impacted individuals. A true and correct copy of the notification letter submitted to all individuals is attached hereto as **Exhibit A**. Further, CSP has taken significant corrective action, including: (1) Changing all passwords for WIFI, cloud storage and network logins; (2) Now requiring MFA for all cloud-based applications; (3) Removing as much sensitive client data from cloud storage as possible; (4) Removing passwords from mobile devices and added password generator and storage app; (5) Ceasing use of email account with admin privileges as daily email account; (6) Creating new email accounts for all staff; (7) Including additional reminders with each email to clients requesting sensitive data be securely uploaded, rather than emailed to CSP; (8) Reviewing network security settings and performed additional penetration testing (9) Improving device-level security; (10) Providing employees with additional training on cyber security threats; (11) Adding Encryption capability to emails; and (12) Adding more sophisticated virus detection software on each workstation.

polsinelli.com

Atlanta	Boston	Chicago	Dallas	Denver	Houston	Kansas City	Los Angeles	Miami	Nashville	New York
Phoenix	St. Louis	San Francisco	Seattle	Silicon Valley	Washington, D.C.	Wilmington				

Polsinelli PC, Polsinelli LLP in California



March 1, 2022

Page 2

If you have any questions or concerns about the Incident, please do not hesitate to contact us.

Sincerely,

Bruce A. Radke

March 1, 2022

Page 3

EXHIBIT A

[Adult 1 Year CM Template]

[Cornelius, Stegent & Price, LLP Letterhead]

<<Name>>

<<Address 1>>

<<Address 2>>

<<City>><<State>><<Zip>>

<<Date>>

Dear <<Name 1>>:

RE: NOTICE OF DATA BREACH

Cornelius, Stegent & Price, LLP and its affiliate Stegent Equity Advisors, Inc. (collectively, “CSP”) values and respects the privacy of your information, which is why we are writing to advise you of an incident that may have involved some of your personal information. We have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft. Nonetheless, we are writing to advise you about the incident and to provide you with guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? On or about September 29, 2021, we discovered that an unknown individual accessed a business email account without authorization. We immediately began measures to limit access to sensitive personal information and retained the services of a specialized cybersecurity firm to help us investigate the Incident. The investigation determined that, while there was no evidence that the unauthorized individual attempted to view or improperly use any of your information, as a result of the Incident, the unauthorized individual would have had access to copy the mailbox data. We immediately reported the Incident to TD Ameritrade and our other key business partners to mitigate the risk of any fraudulent activity.

What Information Was Involved? On about January 12, 2022, we determined that the files contained some of your personal information, including your <<variable text>>.

What We Are Doing. In addition to the actions described above, we have also taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. We are also notifying you of the incident so that you can be aware and take steps to protect yourself. Finally, although we are not aware of any instances of fraud or identity theft resulting from this incident, out of an abundance of caution, we are offering a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary, one-year membership, please see the additional information attached to this letter.**

What You Can Do. While we have no evidence that your personal information has been misused, we encourage you to take advantage of the complimentary credit monitoring included in this letter. You can also find more information on steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* page.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience or concern this incident might

cause. For further information and assistance, please call (833)-593-0150 (toll free) from 9:00 AM - 5:00 PM Central, Monday through Friday.

Sincerely,

Loyd Stegent

ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **05/22/2022** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: **[Code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring 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 should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by 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 can print a copy of the request form at <http://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

District of Columbia Residents: District of Columbia residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the District of Columbia Attorney General's office at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

North Carolina Residents: North Carolina residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 877-566-7226 (Toll-free within North Carolina), 919-716-6000, www.ncdoj.gov.