CP & Co.

Charles Pratt & Company, LLC

December 9, 2025

[redacted]

Dear [redacted]

I am writing to inform you of a recent data security incident experienced by Charles Pratt & Company ("Charles Pratt") that may have affected your personal information. We take the privacy and security of all information within our possession very seriously. Please read this letter carefully, as it contains information regarding the incident and steps that you can take to help protect your information.

What happened:

- At the end of June 2025, a Charles Pratt employee, unfortunately and unknowingly, clicked on a "Phishing" email. This refers to an email that appears to come from a trusted or known source, but clicking on its links allows an unauthorized intruder to access information. In this case, an intruder entered and had access to our email environment for approximately three weeks. During that time, the intruder could read and send messages from one employee's email address.

- The intruder, using the employee's email, drafted an internal email that looked like it was received from a client who instructed us to conduct a funds transfer. The banking details/instructions were new, and the amount was significant. The message also addressed our procedures for such requests, making it appear credible and leading us to make the transfer. The affected client is aware of this situation and has been made whole for the transfer processed on June 26, 2025.

- On July 8, 2025, we became aware that this was a fraudulent transfer. We immediately notified the Federal Bureau of Investigation and our service provider to immediately secure our technology infrastructure.

- The intruder compromised one employee's email. Once we recognized the issue, our technology service provider immediately locked out the intruder. No additional employee emails were compromised.

- We then commenced a search for a forensic cybersecurity firm. Cypfer, a firm that investigates and remediates cyber-attacks, was hired on October 1, 2025.

What was found by Cypfer?

- We received confirmation that the intruder was only able to compromise the one employee's email.

767 Third Avenue, 6th Floor New York, NY 10017-9026
Telephone 212-867-4444 Facsimile 212-867-0028

- However, on November 19, 2025, they discovered that on or about June 23, 2025, the intruder accessed a link (shared via email) to a file containing sensitive client information. This included social security numbers, dates of birth, mailing addresses, and external bank account numbers.

- The forensic team examined our hardware, software, and servers. Recommended enhancements to our routine security protocols have been implemented to better protect our network's security.

What Information Was Involved

As noted above, the information in the file includes one or more of the following fields: your name, social security number, date of birth, mailing address, and external account numbers.

What We Are Doing

As soon as we discovered this incident, we took the mitigation steps described above and implemented measures to enhance security and minimize the risk of a similar incident occurring in the future. We will continue to work with Cypfer on a semi-annual basis.

Charles Pratt is also offering you 2 years of complimentary identity theft protection services through Aura, a leader in consumer identity protection. These services include 24 months of credit monitoring, dark web monitoring, and fully managed identity theft recovery services.

What You Can Do

You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complimentary identity protection services provided by Charles Pratt. We have arranged for you to receive a complimentary two-year membership to Aura. This product helps detect possible misuse of your personal information and provides you with identity protection support. To activate your protection:

- Go to https://aura.com/activate
- **Enter your unique activation code:** [redacted]
- Follow the on-screen instructions to create your account
- Set up protection from your Aura dashboard
- For questions or help with set-up, please call 833-552-2123

Please be aware that Aura will prompt you to enter your own Credit/Debit Card information when setting up your account, solely for renewal purposes beyond the initial two years. If you do not wish to renew your membership after the two years, then please contact Aura at least 30 days prior to your autorenewal.

For More Information

Further information about how to protect your information appears on the following page. If you have questions or need assistance, please call 212-867-4444 Monday through Friday from 9:00 AM to 5:30 PM, and Cynthia Lopez, Peggy Cutter, or I will assist you. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause. Charles

Pratt will continue to work with Cypfer on an ongoing basis to continue to monitor our current environment.

Thank you for your time and attention to this matter. Once again, we apologize for the inconvenience and are available to answer questions.

Regards,

Richard Coster
President and CEO

Encl.

Steps You Can Take to Help Protect Your Personal 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 (the "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 www.annualcreditreport.com, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
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 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 respective 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
877-438-4338

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Maine Attorney General
109 Sewell Street
Augusta, ME 04330
207-626-8800

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.maryland.gov/i-need-to/Pages/identity-theft-information.aspx
888-743-0023

New Jersey Attorney General
PO Box 080
Trenton, NJ 08625
https://www.njoag.gov/
(609) 292-4925

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include: the right 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 www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.