

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700

Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

JORDAN MORGAN

JMorgan@c-wlaw.com

August 20, 2023

Via E-Mail (IDTheft@oag.state.md.us)

Office of the Attorney General

200 St. Paul Place

Baltimore, Maryland 21202

To Whom It May Concern:

We serve as counsel for New York City Criminal Justice Agency (“NYCCJA”), located at 299 Broadway, New York, NY 10007, and provide this notification to your Office of a recent data security incident suffered by NYCCJA. By providing this notice, NYCCJA does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On June 5, 2023, NYCCJA discovered unauthorized access within its payroll system, PayCom. Upon discovery, NYCCJA immediately took steps to secure the system and engaged a third-party team of forensic investigators to determine the full nature and scope of the incident. On June 6, 2023, NYCCJA provided voluntary notice to all current and former NYCCJA employees via email. On June 12, 2023, NYCCJA provided voluntary written notification offering complimentary tri-bureau credit monitoring and dark web monitoring to all current and former NYCCJA employees, which is attached hereto as **Exhibit A**. On July 10, 2023, following a thorough investigation, NYCCJA confirmed that a limited amount of information may have been accessed in connection with this incident. However, at that time, NYCCJA was unaware of any Maryland residents being impacted by this incident.

However, on August 14, 2023, NYCCJA discovered one (1) resident of Maryland whose Social Security number may have been affected by this incident.¹ As our investigation is ongoing, we will provide supplemental notification should we determine additional Maryland residents are potentially affected.

NYCCJA will provide written notice of this incident to the potentially impacted Maryland residents on August 21, 2023, pursuant to Maryland state law. A copy of the notice letter is attached hereto as **Exhibit B**, which provides details of the incident, and steps impacted individuals can take to protect their data.

¹ Please note that the Maryland resident was discovered by NYCCJA’s third-party notification vendor while performing a National Change of Address search.

Please contact me should you have any questions.

Very truly yours,

A handwritten signature in black ink, appearing to read "Jordan Morgan", enclosed within a thin black rectangular border.

Jordan Morgan, Esquire
CIPRIANI & WERNER, P.C.

Exhibit A

Dear [name],

We are writing to provide you with information regarding a data breach that involved the New York City Criminal Justice Agency.

What Happened?

On the morning of June 5, 2023, we discovered that one of the user accounts for our PayCom Payroll and HR Management system had been compromised. Our payroll system contains personal information and banking information of all CJA employees and the account that was compromised had privileges to see personally identifiable information for other users. As a result, your personal information was potentially accessible to unauthorized individuals. We are not aware of any attempted or actual misuse of your information as a result of this data security event. We are providing this notification so that you may take steps to protect your information should you feel it is appropriate to do so.

What Information Was Involved?

The employee information involved included your full name, your social security number, your date of birth, and your complete address.

What Are We Doing?

The New York City Criminal Justice Agency has engaged an identity theft provider (CLC ID Protect) to assist us with helping you protect your information. CLC IDP has put together a preventive resource guide and they will be providing, at no cost to you, free ID theft counseling/restoration, credit and identity monitoring for one year. It is important that you follow the preventative steps and enroll in monitoring as these are the tools that can prevent the thieves from using your information to their financial benefit.

In partnership with CLC ID Protect, we've put together the following resources for you.

1. Preventative Guide – see enclosed Data Breach Preventative Steps
2. Identity Theft Counseling & Restoration – in the event you have questions or need help with protecting or restoring your identity (fraudulent accounts, unauthorized use of your information) you will have free and unlimited access to an ID Theft Fraud Resolution Specialist.
3. Free Tri-Bureau Credit Monitoring for one year
4. SS#, Dark Web and Identity Monitoring for one Year

The second attachment summarizes the services mentioned above in 2.– 4.

How to Access Services:

- Identity Theft Restoration can be access by calling dedicated ID Theft Customer Service Line at (800) 706-5749.
- Credit and ID Monitoring
 - You will need to visit <https://clcidprotect.net/co/nyccja> and click on “sign up.”
 - Enter your Employee ID# (located in PAYCOM w/ no zeros in front) and Last Name
 - Upon authentication you will receive a Welcome Email from CLD ID Protect
 - Access your member portal by following the instructions in the Welcome Email
 - Utilize the member portal to activate your Credit and Identity Monitoring services.

For More Information or Questions.

We will be 2 separate educational webinars addressing how to activate your benefit and preventative steps to address concerns revolving around a data breach. Registrations links will be sent soon to both the 11am and 4pm EST sessions starting on Tuesday, June 13th.

If you have any other questions, or concerns, please feel free to reach out to CLC ID Protection Fraud Resolution Team directly at:

Email Support: idtheft@clcidprotect.net

Phone Support: (800) 706-5749

Sincerely,

The New York Criminal Justice Agency

Exhibit B

<<First Name>> <<Last Name >>
<<Address 1>>
<<City>>, <<State>> <<Zip>>

<<Date>>

Re: ***Important Security Notification. Please read this entire letter.***

Dear <<First Name>> <<Last Name>>:

We previously wrote to you on June 6, 2023 to inform you of a data security incident experienced by the New York City Criminal Justice Association (“NYCCJA”) that may have impacted some of your personal information described below. Please note that this letter is a follow up letter to the same incident and is meant to provide you with additional information about steps that can be taken to help protect your information

We take the privacy and security of all information very seriously. While we have no evidence to suggest that any information was subject to actual or attempted misuse as a result of this incident, we are taking steps to proactively notify potentially impacted individuals out of an abundance of caution.

What Happened:

On June 5, 2023, NYCCJA discovered unauthorized access within its payroll system, PayCom. Upon discovery, NYCCJA immediately took steps to secure the system and engaged a third-party team of forensic investigators to determine the full nature and scope of the incident. On July 10, 2023, following a thorough investigation, NYCCJA confirmed that a limited amount of information may have been accessed in connection with this incident.

At this time, there is no indication that any information has been misused. However, we are providing this notification to you out of an abundance of caution and so that you may take steps to safeguard your information if you feel it is necessary to do so.

What Information Was Involved:

It is important to note, as mentioned above, that there is no evidence to suggest that any information has been misused. The information that could have been accessed by the unauthorized individual(s) may have included your first name or initial and last name, in combination with your Social Security number.

What Are We Doing:

NYCCJA has taken every step necessary to address the incident and is committed to fully protecting all of the information that you have entrusted to us. Upon learning of this incident, we immediately secured the system, reset passwords, and took steps to enhance the security of all information to help prevent similar incidents from occurring in the future.

Credit Monitoring:

In the previous letter, NYCCJA offered for you to enroll, at no cost to you, in twelve (12) months of identity theft protection services through CLC ID Protect. CLC ID Protect identity protection services include: **twelve (12) months** of tri-bureau credit monitoring and dark web monitoring and fully managed identity theft recovery services. If you have any questions about those services, or if you would like additional information in enrolling in those services, please do not hesitate to contact us at (646)-213-2600. Due to privacy laws, we cannot activate these services for you directly.

What You Can Do:

In addition to enrolling in the complimentary credit monitoring service detailed within, we recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change your password, take additional steps to protect your account, and notify your financial institution or company if applicable. Additionally, please report any suspicious incidents to local law enforcement and/or your State Attorney General. You can also review the enclosed “*Steps You Can Take to Help Protect Your Information*” for additional resources.

For More Information. Should you have additional questions or concerns regarding this matter, please do not hesitate to contact us at (646)-213-2600. You can also write us at 299 Broadway, New York, NY 10007.

Sincerely,

Crystal Cotton
Chief of People and Culture Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card);
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.