

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

Amanda Ruggieri
ARuggieri@c-wlaw.com

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

July 19, 2024

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

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

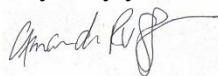
We serve as counsel for ADD Systems located at 6 Laurel Drive Flanders, NJ 07836 and write to inform you of two data security incidents. By providing this notice, ADD Systems does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On March 21, 2024, ADD Systems discovered a network disruption that limited its ability to access certain systems. Upon discovery, ADD Systems immediately took steps to secure the network and engaged a third-party forensic firm to investigate the incident. Thereafter, on May 14, 2024, while the investigation into the first incident was still ongoing, ADD Systems discovered a second network disruption. ADD Systems again took steps to secure the network and engaged a third-party forensic firm to investigate the incident. On May 31, 2024, following a full and thorough investigation, ADD Systems determined that a limited amount of information related to current and former employees may have been accessed by an unauthorized third party in connection with these incidents. On July 16, 2024, ADD Systems confirmed that one (1) Maryland resident may have been affected. The impacted information was limited to the individual's first and last name in combination with Social Security number, driver's license number, bank account information, and/or other form of identification used to complete an I9 form.

On July 19, 2024, ADD Systems sent written notice of this incident to the potentially impacted Maryland resident pursuant to Maryland state law. The notice letter included an offer of complimentary credit monitoring and identity protection services for twelve (12) months. The notice letter sent to the individual is substantially similar to the letter attached hereto as Exhibit "A."

If you have any questions, please contact me.

Very truly yours,



Amanda Ruggieri, Esquire
CIPRIANI & WERNER, P.C.

Exhibit A



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

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

<<b2b_text_1 (RE: [Letter Header]. Please read this entire letter.)>>

Dear <<first_name>> <<last_name>>:

ADD Systems writes to notify you of two incidents that may have impacted some of your personal information described below. We take the privacy and security of information in our care very seriously. At this time, there is no evidence to suggest that any information has been fraudulently misused. However, out of an abundance of caution, we are providing you information about these incidents, our response, and steps you can take to help protect your information, should you feel it is appropriate to do so.

What Happened:

On March 21, 2024, we discovered a network disruption that limited our ability to access certain systems. Upon discovery, we immediately took steps to secure the network and engaged a third-party forensic firm to investigate the incident. Thereafter, on May 14, 2024, while the investigation into the first incident was still ongoing, we discovered a second network disruption. We again took steps to secure the network and engaged a third-party forensic firm to investigate the incident. On May 31, 2024, following a full and thorough investigation, we determined that a limited amount of information related to current and former employees, kept in the normal course of business, may have been accessed by an unauthorized third party in connection with these incidents.

What Information Was Involved:

The potentially accessed information may have included your first name or initial and last name, in combination with your Social Security number, driver's license number, bank account information, and/or other form(s) of identification used to complete your I9 form.

What We Are Doing:

We have taken steps to address the incident and are committed to protecting personal information in our care. Upon learning of this incident, we immediately took steps to secure our network and undertook a thorough investigation.

As an additional safeguard, we have arranged for you to activate, at no cost to you, an online Identity Monitoring service for <<Monitoring Term Length (Months)>> months provided by Kroll. Due to state and federal privacy laws, we cannot activate you directly. If you wish to take advantage of this complimentary identity monitoring service, you must activate yourself.

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, notify your financial institution or company if applicable, and take any additional steps needed to protect your account. Additionally, please report any suspicious incidents to local law enforcement and/or your state Attorney General. Please 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 our dedicated call center at (866) 810-1447, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays. You can also write us at 6 Laurel Drive Flanders, NJ 07836.

We take the security of information entrusted to our care very seriously. While we sincerely regret this potential exposure occurred, please be assured that we are taking appropriate actions to rectify the situation and prevent such incidents in the future.

Sincerely,

Bruce Carl Bott, President

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<Monitoring Term Length (Months)>> months. 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, 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.



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.

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.

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 some or all of 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. Social Security card, pay stub, or W2; and
8. 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 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 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. There are 16 Rhode Island residents impacted by this incident.