

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

JASON M. GOODWIN
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

NICHOLAS J. MARTIN
nmartin@c-wlaw.com

Telephone: (610) 567-0700
Fax: (610) 567-0712

November 30, 2023

Via Email

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

RE: Data Breach Notification

To Whom It May Concern:

We serve as counsel for INX International Ink Co. ("INX") located at 150 N. Martingale Rd, Suite 700, Schaumburg, Illinois 60173 and write to provide notice of a recent IT security incident. By providing this notice, INX does not waive any rights or defense under Maryland law including the data breach notification statute.

On July 21, 2023, INX discovered an IT security incident that resulted in unauthorized access to certain INX systems. Upon discovery, INX took immediate steps to secure the network and systems. Further, INX retained outside legal counsel and outside forensic specialists to assist in a thorough investigation into the nature and scope of the incident. The investigation confirmed that an unauthorized actor gained access to INX systems. There is no direct evidence that personal information left the INX network. However, out of an abundance of caution, INX engaged in a thorough review of the at-risk data to determine the types of information at risk and to whom the information relates. On or around October 20, 2023, INX completed its initial review and identified limited personal information which may have been impacted. While INX does not have any evidence of misuse, or threat of misuse of any personal information, INX subsequently worked to obtain up-to-date contact information to provide individuals with direct notification in an abundance of caution. This process, including a National Change of Address ("NCOA") search, was completed on November 27, 2023. Upon completion of the NCOA, INX confirmed that this incident potentially affected information relating to twelve (12) Maryland residents, including their first and last name, date of birth, and Social Security number.

In response to this incident, INX took steps to secure their environment, conducted a thorough investigation and notified law enforcement. Additionally, INX began providing notice to the potentially impacted individuals on November 30, 2023, via U.S. mail. A copy of the notice is attached as ***Exhibit A***. In an abundance of caution, INX is offering potentially impacted individuals complimentary credit monitoring and identity theft protection services for 12 months.

Very truly yours,

CIPRIANI & WERNER, P.C.

By:



Jason M. Goodwin, Esq.

Exhibit A

INX International Ink Co.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-08164 1-1



<<Name>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>



Important Notice

Dear [first name] [last name],

We are writing to inform you of a recent incident experienced by INX International Ink Co. (INX) which may have impacted certain information we hold on INX systems. We take this incident very seriously and are providing you information about the incident, our response, and steps you can take to protect your information out of an abundance of caution.

What Happened? On July 21, 2023, INX discovered suspicious activity associated with certain INX systems. We immediately began an investigation, which included working with third-party specialists and legal counsel to assist in our investigation and to determine the nature and scope of the activity. Our investigation determined an unknown party was able to access parts of our IT network. Having investigated the actions of the unauthorized party, we have not seen any definitive evidence that any personal information has left our network. However, we conducted a review to determine the information potentially at risk and are notifying you as a precaution so you can take steps to protect your data. On October 20, 2023, this review was completed, and we worked to provide you with notice as soon as possible.

What Information Was Involved? The information potentially impacted during the incident may have included your name in combination with one or more of the following data elements: <<Data Elements>>. Please note that we have no evidence of misuse of this information but are notifying you out of an abundance of caution.

What We Are Doing. In response to this incident, we immediately took steps to secure our environment and undertook a thorough investigation. We have also implemented additional technical safeguards to further enhance the security of information in our possession. Additionally, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring services at no charge. These services provide you with alerts for <<12/24>> months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do. We encourage you to enroll in the credit monitoring and identity protection services we are making available to you. Instructions about how to enroll in these services and additional resources available to you are included in the enclosed *Steps You Can Take to Protect Your Information*.

For More Information: Should you have any questions or concerns regarding this incident, please contact our dedicated assistance line at 1-833-660-0245 Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern time (excluding major U.S. holidays).

Sincerely,

INX International Ink Co.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

To enroll in Credit Monitoring services at no charge, please log on to <<URL>> and follow the instructions provided. When prompted please provide the following unique code to receive services: <<UNIQUE CODE>> In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements 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); and
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.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and <https://www.marylandattorneygeneral.gov>. INX may be contacted at 150 N. Martingale Rd, Suite 700, Schaumburg, IL 60173.

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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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 https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 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 contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>. INX may be contacted at 150 N. Martingale Rd, Suite 700, Schaumburg, IL 60173.