

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

HILARY HIGGINS
hhiggins@c-wlaw.com

JORDAN MORGAN
jmorgan@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

April 8, 2022

Via Email (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Security Breach Notification

To Whom It May Concern:

I serve as counsel for Apis Services, Inc. ("Apis"), located at 120 Prospect Street, Reading, PA 19606. We write to provide notification of a recent data security incident. By providing this notice, Apis does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On November 9, 2021, Apis became aware of a potential network intrusion that impacted some of their systems. Upon discovery, Apis immediately secured its network and engaged a third-party forensic firm to investigate the incident. On February 21, 2022, after a thorough investigation, Apis confirmed that a limited amount of personal information may have been impacted by this event and identified the potentially affected individuals. However, Apis was missing contact information for a significant amount of impacted individuals at that time. As a result, Apis immediately engaged in a thorough review of its internal records to identify contact information for all affected individuals.

Apis completed its record review and address search on March 7, 2022, and at that time, discovered that thirty-five (35) residents of Maryland may have been affected by this incident. As our investigation is ongoing, we will provide supplemental notification should we determine additional residents of Maryland are potentially affected.

Apis will notify the potentially impacted individuals on April 8, 2022, via First Class Mail and is offering the affected Maryland residents complimentary credit monitoring for 12 months.

A copy of the draft notification letter is attached as **Exhibit A**. The letter outlines the incident and provides potentially affected individuals with additional resources to protect their identity and monitor their credit history and personal accounts. Apis is taking proactive steps to ensure that all state and federal notification obligations are complied with due to this incident.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

A handwritten signature in blue ink, appearing to read 'Hilary Higgins', with a stylized flourish at the end.

Hilary Higgins, Esq.

EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

April 8, 2022

H7762-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 GENERAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



RE: [Variable Header]

Dear Sample A. Sample:

Apis Services, Inc. (“Apis”) writes to notify you of a recent incident that may have impacted some of your personal information described below.

We take the privacy of information in our care seriously, and while we have no evidence to suggest that any information was misused, in an abundance of caution, we are providing you information about the incident, our response, and steps you can take to protect your information.

What Happened:

On or around November 9, 2021, Apis fell victim to a network intrusion that affected some of our systems. Upon discovery, we immediately secured our network and engaged a third-party forensic firm to investigate the nature and scope of the incident. On February 21, 2022, we discovered that a limited amount of information may have been accessed by an unauthorized third party in connection with this incident.

At this time, there is no indication that any information has been misused. However, Apis is 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 and last name, in combination with your [data elements].

What We Are Doing:

Apis has taken steps to address the incident and is committed to protecting personal information in its care. Upon learning of this incident, Apis immediately took steps to secure its systems, and to enhance the security of its network to prevent similar incidents from occurring in the future.

0000001



H7762-L01

Credit Monitoring:

As an additional safeguard for your information, Apis has arranged for you to enroll in a complimentary ## month membership of Experian's® IdentityWorksSM. Due to State and Federal privacy laws, however, Apis cannot enroll you directly and if you wish to take advantage of this complimentary credit monitoring service, you must enroll yourself. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: July 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

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 (833) 468-0640 by **July 31, 2022**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

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 and 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. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

Should you have questions or concerns regarding this matter, please do not hesitate to contact us at (833) 468-0640, or write us at 120 Prospect Street, Reading, PA 19606.

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

Sincerely,

Thomas S. Papa
Chief Executive Officer

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Additional Details Regarding Your ## Month Experian Identityworks Membership:

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

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 file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** 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.

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); 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.

* 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.



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 www.oag.state.md.us.

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 are 3 Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>.