



900 W. 48th Place, Suite 900, Kansas City, MO 64112 • 816.753.1000

October 26, 2023

Alexander D. Boyd
816-572-4470
816-753-1536
aboyn@polsinelli.com

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General

Attn: Jeff Karberg, Administrator of the Identity Theft Program

Attn: Security Breach Notification

200 St. Paul Place

Baltimore, MD 21202

Re: Notification of Data Security Incident

Dear Madam/Sir:

We represent It Works Marketing, Inc. ("It Works"), 908 Riverside Dr., Palmetto, FL 34221, in connection with an incident that involved the personal information of certain Maryland residents. It Works is reporting the incident pursuant to MD. CODE ANN., COM. LAW § 14-3504(h). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While It Works is notifying you of this incident, It Works does not waive any rights or defenses relating to the incident, this notice, or the applicability of Maryland law on personal jurisdiction.

NATURE OF THE INCIDENT

On May 4, 2023, It Works employees discovered that files on company servers were encrypted. Employees also discovered a ransom note. Upon discovering the incident, It Works promptly began an internal investigation, worked to secure its systems, and notified law enforcement. It Works, through its counsel, also engaged an outside forensic firm to respond to and investigate the incident. The forensic investigation determined that an unknown third party accessed It Works' systems from May 2, 2023, until May 4, 2023. The forensic investigation of the available data did not identify evidence that the third party accessed or acquired any data as a part of the Incident. However, the third party ultimately posted data that it stole from It Works on the third party's leak site. It Works, through its forensic security firm, downloaded and reviewed data posted by the third party. On September 21, 2023, the forensic firm completed its review and determined that the acquired files contained the personal information for certain individuals.



October 26, 2023

Page 2

The information acquired by the third party includes individuals' names, dates of birth, and/or Social Security numbers. At this point, It Works is not aware of any fraud or identity theft to any individual as a result of this incident.

NUMBER OF RESIDENTS NOTIFIED

It Works conducted a comprehensive review of the acquired information. On September 21, 2023, It Works determined that the personal information of three (3) Maryland residents were involved in the incident. It Works is notifying the three (3) Maryland residents today, October 26, 2023. The notification letter includes an offer for twelve (12) months of complimentary credit monitoring and identity theft protection. Enclosed is a copy of the notice that is being sent to the residents via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, It Works promptly controlled the incident by preventing further access to its computer system. It also engaged a forensic security firm to investigate and confirm the security of its computer systems. It Works is undertaking efforts to reduce the risk of a similar incident occurring in the future, including enhancing its technical security measures. Finally, as discussed above, It Works is notifying the potentially involved individuals, providing free credit monitoring services as appropriate, and providing individuals with information on how they can protect themselves against fraudulent activity and identity theft.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Alexander D. Boyd

Enclosure



<<Name>>

<<Address 1>>

<<Address 2>>

<<City>><<State>><<Zip>>

<<Date>>

RE: NOTICE OF DATA BREACH

Dear <<Name 1>>:

It Works Marketing, Inc. values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that involved some of your personal information.

What Happened? On May 4, 2023, we discovered that an unknown, unauthorized third party encrypted some of our files. Upon learning of the incident, we promptly contained the incident, notified law enforcement, and engaged a forensic security firm to investigate and confirm the security of our computer systems. The forensic investigation determined that an unknown third party accessed our systems from May 2, 2023 until May 4, 2023. The forensic investigation of the available data did not identify evidence that the third party accessed or acquired any data. However, we later discovered that third party did acquire certain files from our computer systems during the incident.

What Information Was Involved? Through our forensic security firm, we reviewed the files acquired by the third party to determine if they contained any personal information. On September 21, 2023, we completed our review and determined that the files contained information that included your [data elements].

What We Are Doing. In addition to the actions described above, we have taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. Although we are not aware of any instances of fraud or identity theft involving your information, we are also offering a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on prompt identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you, and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

What You Can Do. We encourage you to take advantage of the complimentary credit monitoring included in this letter. You can also find more information on steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call (941)799-6769 from 9 a.m. – 5 p.m. Eastern, Monday through Friday, or email privacy@itworks.com.

Sincerely,

A handwritten signature in blue ink, appearing to read 'T. Seat'.

Tim Seat
General Counsel
It Works Marketing, Inc.

ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [REDACTED] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: [Code]

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 877-288-8057. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

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, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** 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.

Activate your membership today at <https://www.experianidworks.com/3bcredit>
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* 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.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring 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 should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by 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 can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze can be placed without any charge and is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Rhode Island Residents: We believe that this incident affected 1 Rhode Island resident. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.