

February 10, 2023

VIA E-MAIL: Idtheft@oag.state.md.us

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

Re: Notification Pursuant to Md. Code Com. Law § 14-3501 *et seq.*

Dear Attorney General Frosh:

We are writing on behalf of our client, Ideal Image Group of Maryland, PC ("Ideal Image"), to notify you of a security incident involving fourteen (14) Maryland residents.

NATURE OF THE INCIDENT

Ideal Image recently learned that Ideal Image sales personnel may have sent digital acknowledgments for service agreements containing customer personal information and information related to future Ideal Image services to sales personnel's personal email.

Upon learning of the issue, Ideal Image immediately commenced a comprehensive internal review, including reviewing employee emails, analyzing employee activity, and conducting employee interviews. Based on the internal review, Ideal Image concluded that this was an isolated practice by a limited number of Ideal Image sales personnel and involved a small number of Ideal Image customers. Based on its review, on January 9, 2023, Ideal Image determined that certain emails going to sales personnel's personal email accounts may have contained Maryland residents' full names and information relating to future medical treatment at Ideal Image.

STEPS WE ARE TAKING RELATED TO THE INCIDENT

Ideal Image has no indication that any of the information has been or will be misused. Ideal Image's review found no evidence of fraud, identity theft, or intent to disseminate personal information beyond sales personnel's personal email, rather it appears that the primary intent was to assist customers with completing and submitting the required paperwork.

Nevertheless, out of an abundance of caution, on February 10, 2023, Ideal Image notified potentially affected Maryland residents of the incident by mail or, if a mailing address was unknown, by email. Enclosed is a sample copy of the notice that was sent to the individuals. Within the letter,

AUSTIN
BOSTON
CHICAGO
DALLAS
DENVER

DETROIT
HOUSTON
JACKSONVILLE
LOS ANGELES
MADISON

MEXICO CITY
MIAMI
MILWAUKEE
NEW YORK
ORLANDO

SACRAMENTO
SALT LAKE CITY
SAN DIEGO
SAN FRANCISCO
SILICON VALLEY

TALLAHASSEE
TAMPA
WASHINGTON, D.C.
BRUSSELS
TOKYO



FOLEY & LARDNER LLP

February 10, 2023

Page 2

Ideal Image provided the Maryland residents with precautionary measures regarding identity and medical theft protection. Although Social Security numbers were not impacted in this incident, Ideal Image has elected to provide the affected Maryland residents with credit monitoring and identity protection services through Experian, at no charge for twelve (12) months, and will staff a support line to answer any questions individuals may have about this incident and the services available to them.

At Ideal Image, protecting the privacy of personal information is a top priority. To help prevent an incident like this from happening in the future, Ideal Image has taken disciplinary action and re-educated its team on the correct data handling procedures and the importance of protecting personal information and implemented additional mandatory training. Furthermore, Ideal Image has instructed the sales personnel to permanently delete and not save, forward, or otherwise disseminate any customer information sent to sales personnel's personal email. Ideal Image continually evaluates and modifies its practices and internal controls to enhance the security and privacy of the personal information it maintains.

If you have any further inquiries concerning this notification, please do not hesitate to contact me.

Sincerely,

A handwritten signature in blue ink, appearing to read 'A. Maguregui', written over a light blue rectangular background.

Aaron T. Maguregui
Foley & Lardner LLP

Encl: Sample Notification Letter



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

February 10, 2023

J0178-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 EXHIBIT C - STANDARD

APT ABC

123 ANY STREET

ANYTOWN, ST 12345-6789



Dear Sample A. Sample:

At Ideal Image, we value and respect the privacy of your information, which is why we are writing to inform you of a recent incident involving the disclosure of your information to the personal email of Ideal Image sales personnel attempting to assist with the purchase of Ideal Image services. Although we have no evidence to suggest that your information has been or will be misused in any way, we are notifying you out of an abundance of caution.

WHAT HAPPENED?

We recently learned that Ideal Image sales personnel may have sent digital acknowledgments for service agreements containing customer personal information and information related to future Ideal Image services to sales personnel's personal email. Upon learning of the issue, we immediately initiated an internal review.

WHAT INFORMATION WAS INVOLVED?

Based on our investigation, by January 9, 2023, we determined that email going to sales personnel's personal email may have contained your full name and information relating to future medical treatment at Ideal Image. Please note, your Social Security Number and financial information were **not** involved.

WHAT WE ARE DOING

Upon learning of this issue, we commenced a comprehensive internal review, including reviewing employee emails, analyzing employee activity, and conducting interviews. We have concluded from the investigation that this was an isolated practice and involved a small number of Ideal Image customers. We found no evidence of fraud, identity theft, or intent to disseminate personal information beyond sales personnel's personal email, and it appears that the primary intent was to assist customers with completing and submitting the required paperwork. Nevertheless, to help prevent an incident like this from happening in the future, we have taken disciplinary action and have re-educated our team on the correct data handling procedures and the importance of protecting personal information. Furthermore, we have instructed sales personnel to permanently delete and not save, forward, or otherwise disseminate any customer information sent to sales personnel's personal email.

Although we have no evidence to suggest that your information has been or will be misused, we are notifying you out of an abundance of caution. To help relieve any concerns following this incident, we have arranged to make available to you 12 months of identity theft protection services provided by Experian® IdentityWorksSM, at no charge. These services include comprehensive credit monitoring and identity restoration services by Experian, one of the three nationwide credit reporting companies. To sign up for this service, please follow the instructions attached to this notice.

0000001



WHAT YOU CAN DO

Although you are not required to take any action, as a general matter, the following practices can help to protect your medical information.

- Review your receipts and billing statements, which you can request from your health care provider. Follow up with your health care provider for any items you do not recognize.
- Ask your health care provider for a current year-to-date report of all services paid for you as a patient. Follow up with your health care provider for any items you do not recognize.
- Only share your health and other personal information with your health care providers and other family members who help you with your medical care.

Although information going to sales personnel's personal email does not affect your credit and we have no evidence to suggest that your information has been or will be misused, we are required by law to provide you certain information about identity theft. Please review the enclosed "Additional Resources" document included with this letter for further steps you can take to protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. It is also recommended that you remain vigilant for potential incidents of fraud and identity theft by reviewing your account statements and monitoring your credit reports for unauthorized activity.

FOR MORE INFORMATION

For further information and assistance, please call our customer service line at **(833) 559-2450** between 8 a.m. - 10 p.m. CST weekdays; and 10 a.m. – 7 p.m. CST Saturday and Sunday.

Sincerely,

Ideal Image

ADDITIONAL RESOURCES
Enrolling in Experian's® IdentityWorksSM

Activate IdentityWorks In Four Easy Steps

- Ensure that you **enroll by: May 31, 2023** (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) 559-2450** by **May 31, 2023**. 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
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 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.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **(833) 559-2450**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* 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.



Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert. You may want to consider placing a fraud alert on your credit report by contacting any of the three nationwide credit reporting agencies identified above. An initial fraud alert is free and will stay on your credit file for at least 90 days. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three (3) major consumer reporting agencies listed above. To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

1-800-349-9960

<https://www.equifax.com/personal/credit-report-services/>

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

<https://www.experian.com/freeze/center.html>

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

1-888-909-8872

<https://www.transunion.com/credit-freeze>

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five (5) years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or up to three (3) business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three (3) credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to remove the security freeze.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC, proper law enforcement authorities and/or your state attorney general. You may also contact these agencies for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-FTC-HELP (382-4357). You may also wish to review the tips provided by the FTC on how to avoid identity theft. A copy of *Taking Charge: What to Do if Your Identity is Stolen*, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at www.ftc.gov/bcp/edu/microsites/idtheft/.

- **For District of Columbia Residents:** You may obtain additional information about identity theft prevention and protection from the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, <https://oag.dc.gov>.
- **For Maryland Residents:** You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1- 410-576-6491 or 1-888-743-0023
- **For Oregon Residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at <https://doj.state.or.us>, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.
- **For Rhode Island Residents:** You have the right to file and obtain a copy of any police report. You also have the right to request a security freeze as described above. You may contact the Rhode Island Attorney General at <https://www.riag.ri.gov>, by calling 401-274-4400, or by writing to 150 South Main Street, Providence RI 02903. There are four Rhode Island residents potentially impacted by this incident.

