



Baker&Hostetler LLP

11601 Wilshire Boulevard
Suite 1400
Los Angeles, CA 90025-0509

T 310.820.8800
F 310.820.8859
www.bakerlaw.com

M. Scott Koller
direct dial: 310.979.8427
mskoller@bakerlaw.com

December 13, 2022

VIA EMAIL (IDTHEFT@OAG.STATE.MD.US)

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

Re: Incident Notification

Dear Attorney General Frosh:

We are writing on behalf of our client, InfoCision Management Corporation (“IMC”), and their customer, Special Olympics, to notify your office of a cybersecurity incident that involved one Maryland resident’s information. IMC is located at 325 Springside Drive, Akron, Ohio 44333.

On September 30, 2022, IMC detected unauthorized access to their corporate network involving encryption of data and systems on the network. Upon discovering the incident, IMC took steps to secure the network, notified law enforcement and launched an investigation. The investigation determined that an unauthorized party accessed IMC’s network beginning on September 19, 2022. The investigation also identified certain files that were taken by the unauthorized party between September 22, 2022, and September 26, 2022.

IMC reviewed the files that were taken to determine if any of the files included personal information. On October 25, 2022, IMC determined that the files included the names and credit or debit card numbers of two Maryland residents.

IMC is mailing a notification letter via First Class mail to the Maryland resident in accordance with Md. Code Ann., Com. Law § 14-3504.¹ A sample of the notification is enclosed.

¹ This report is not, and does not constitute, a waiver of IMC’s objection that Maryland lacks personal jurisdiction over the company related to this matter.

December 13, 2022

Page 2

IMC has also established a dedicated, toll-free call center that individuals can call to obtain more information regarding the incident.

To reduce the risk of a similar incident from occurring in the future, IMC has changed passwords and implemented additional security measures and controls within the corporate network.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink that reads "M. Scott Koller". The signature is written in a cursive, flowing style.

M. Scott Koller
Partner

Enclosure



John Smith
123 Main Street
Akron, OH 44333

December 12, 2022

Dear John Smith:

InfoCision Management Corporation is a telemarketing firm who works on behalf of Special Olympics to educate supporters about the mission and to make a donation to the organization. We are writing to you today to notify you of a data security incident that involved some of your personal information that you provided when donating to Special Olympics in the past. We sincerely apologize that this incident occurred and are taking every step to notify those potentially impacted and make sure this doesn't happen again in the future. This notice explains the incident, measures we have taken and some additional steps you can take in response.

What Happened?

On September 30, 2022, our IT team identified a data security incident involving unauthorized access to our corporate network. Upon discovery, we immediately took steps to secure the network, notify law enforcement and began an investigation with the assistance of an outside cybersecurity firm. Our investigation determined that an unauthorized party accessed some data stored on our network between September 22, 2022, and September 26, 2022.

What Information Was Involved?

We reviewed the accessed data and on October 25, 2022, we determined the information included some of your personal information. The accessed data included your name and payment card number or financial account number ending in 1234.

What We Are Doing.

We assure you that we take this incident very seriously. To help prevent a similar incident in the future, we have changed passwords and implemented additional security measures and controls in our network.

What You Can Do.

For more information, as well as some additional steps you can take to help protect yourself, please see the pages that follow this letter.

For More Information.

We sincerely regret any inconvenience caused by this incident. If you have any questions, please call 844-728-1097, Monday through Friday, between 9:00 am and 5:00 pm, Eastern Time, Monday through Friday.

Sincerely,

Jeffrey R. Mellen

Jeffrey R Mellen, Director of Information Security



ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will

also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

InfoCision Management Corporation, 325 Springside Drive, Akron, Ohio 44333 | (330) 668-1400

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

North Carolina: You may contact and obtain information from your state attorney general at: North Carolina Attorney General's Office, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov