



Richard Goldberg, Partner & Vice-Chair
Cybersecurity & Data Privacy Team
1650 Market Street, Suite 3600
Philadelphia, PA 19103
rgoldberg@constangy.com
Mobile: 917.744.1760

February 14, 2023

VIA EMAIL: ldtheft@oag.state.md.us

Attorney General Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566

Re: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents Michael & Son Services Inc. ("Michael & Son"). Michael & Son experienced a suspected cyber event described in greater detail below. While a forensic investigation did not definitively prove access to sensitive information, Michael & Son has provided notice of the event to individuals who may have been involved. The company also provided resources and information for individuals to protect their personal information.

1. Nature of the Security Incident

On December 15, 2022, Michael & Son discovered unauthorized activity on its systems. In response, Michael & Son immediately took steps to terminate the activity and to secure its network, systems, and data. It also retained independent cybersecurity experts to conduct a forensic investigation into the incident and determine what happened.

The forensic investigation was unable to conclusively determine whether there was unauthorized access to files stored within Michael & Son systems, including those that store personal information. Out of an abundance of caution, Michael & Son then worked diligently to identify individuals whose information could have been impacted, as well as their current address information to notify all potentially impacted individuals about the incident. That process was completed on January 18, 2023.

To date, Michael & Son has no reason to believe that personal information of potentially impacted individuals has been misused as a result of this incident. Out of an abundance of caution, Michael & Son is notifying all potentially impacted individuals of the incident, providing them with steps they can take to protect their personal information, and offering them free credit and identity monitoring services.

2. Number of Affected Maryland Residents & Information Involved

The incident may have involved personal information for approximately 940 Maryland residents. The potentially impacted information involved in the incident may differ depending on the individual but may include the following for affected Maryland residents: name in combination with Social Security number, as well as driver's license and passport number if those were provided by the individual to Michael & Son. Again, Michael & Son has no reason to believe that the information involved has been or will be published, shared, or otherwise misused.

3. Notification to Affected Individuals

On February 14, 2023, notification letters will be sent to affected Maryland residents by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers complimentary identity protection services to each individual whose Social Security numbers was affected by this event, including credit monitoring, dark web monitoring, \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter is enclosed.

4. Measures Taken to Address the Incident

In response to the incident, Michael & Son retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Michael & Son has implemented additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future.

Finally, Michael & Son is notifying the potentially affected individuals and providing them with steps they can take to protect their personal information as discussed above and reporting the incident to nationwide consumer reporting agencies (i.e., Equifax, Experian, and Transunion).

5. Contact Information

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at RGoldberg@constangy.com or 917.744.1760.

Sincerely,



Richard Goldberg of
Constangy, Brooks, Smith & Prophete LLP

RG:mff

Encl.: Sample Notification Letter

cc: Michael F. Ferragamo, Constangy (MFerragamo@constangy.com)



Return Mail to: IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-903-3648

Or Visit:

<https://app.idx.us/account-creation/protect>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

February 14, 2023

Notice of Data Security <<Variable 2>>

Dear <<First Name>> <<Last Name>>,

We are informing you of a data security incident that may have involved your personal information. Michael & Son takes the security of personal information in its care very seriously. This notice explains the incident, provides you with steps you can take to protect your information, and offers you complimentary credit monitoring and identity protection services.

What happened? On January 18, 2023 we determined that your information may have been impacted by a data security incident. On December 15, 2022, we detected unusual activity in our systems. We immediately shut down some systems and began an investigation with the help of third-party cybersecurity experts. It was eventually determined that an unauthorized person may have gained access to some personal information, including current employees. Please note that we have no reason to believe that your information has been misused as a result of this incident. Regardless, out of an abundance of caution, we are notifying you and providing you with free credit monitoring and information you can take to protect your data.

What Information Was Involved? The data involved may have included your name in combination with your Social Security number (and driver's license and passport number if you provided those to us).

What We Are Doing: In addition to the steps described above, we are working with cybersecurity experts to help prevent a similar incident from occurring in the future. We are also offering you complimentary identity theft protection services through IDX. These services include: <<12 months/24 months>> of credit and dark web monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do: We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-903-3648 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is May 14, 2023. Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take advantage of this offering.

For More Information: You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Michael & Son Services, Inc.
5740 General Washington Drive | Alexandria, Virginia 22312

Please call 1-833-903-3648 or go to <https://app.idx.us/account-creation/protect> for help or for any questions you may have.

The privacy and security of your information is very important to us. We take this incident very seriously and we regret any worry or inconvenience this may cause you.

Sincerely,

Michael & Son Services, Inc.

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and 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 also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

