



Matthew Toldero, Partner
Cybersecurity & Data Privacy Team
One West 4th Street, Suite 850
Winston-Salem, NC 27101
mtoldero@constangy.com
Mobile: 336.448.8552

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

May 28, 2024

VIA ONLINE SUBMISSION

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Tel: 410-576-6491
Email: Idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Attorney General Anthony G. Brown:

We represent Information Network Associate, Inc. (“INA”) located at 5235 North Front Street Harrisburg, Pennsylvania 17110, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. By providing this notice, INA does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

1. Nature of the Data Event

On February 9, 2024, an INA employee mistakenly emailed employee forms to someone outside the organization. Upon discovery, INA quickly launched an investigation into the nature and scope of this event. The investigation confirmed that the email included three files containing 2023 W-2 forms for INA employees. There is no evidence of any access to any INA computers, systems or accounts, which remain secure. INA believes this was isolated to a single email sent in error.

The information that could have been subject to unauthorized access includes first and last name, as well as Social Security number.

2. Notice to Maryland Residents

On or about May 24, 2024, INA provided written notice of this incident to one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

3. Other Steps Taken and To Be Taken

Upon discovering the event, INA moved quickly to investigate and respond to the incident, assess the security of INA systems, and identify potentially affected individuals. INA is also working to implement additional safeguards and training to its employees. INA is providing access to credit monitoring services for twelve (12) months, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, INA is providing impacted individuals with guidance on how to better protect against identity theft and fraud. INA is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

4. Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 336.448.8552.

Sincerely,

A handwritten signature in dark ink, appearing to read "Matt Toldero". The signature is fluid and cursive, with the first name "Matt" and last name "Toldero" clearly distinguishable.

Matt Toldero
Partner

Exhibit A



P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code:<<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

May 24, 2024

Notice of Data Breach

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

I am writing to notify you of a recent event experienced by Information Network Associates (“INA”) that may have impacted your personal information. INA takes the privacy and security of all personal information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened? On February 9, 2024, an INA employee mistakenly emailed employee forms to someone outside our organization. Upon discovery, we quickly launched an investigation into the nature and scope of this event. Our investigation confirmed that the email included three files containing 2023 W-2 forms for INA employees. There is no evidence of any access to any INA computers, systems or accounts, which remain secure, and we believe this was isolated to a single email sent in error.

What Information Was Involved? The information potentially impacted in connection with this incident included your name as well as your Social Security number.

What Are We Doing? As soon as INA discovered this incident, INA took the steps described above. In addition, INA implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future.

As we value our current and former employees, we are providing you with information about steps that you can take to help protect your personal information and as well as complimentary identity protection services through IDX – a data breach and recovery services expert. These services include 12 months of credit¹ and dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The enrollment instructions for the complimentary monitoring and identity protection services, which includes 12 months of Credit and CyberScan Dark Web monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services are below.

The deadline to enroll in these services is August 24, 2024. With this protection, IDX will help to resolve issues if your identity is compromised.

¹ To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

What You Can Do: You can follow the recommendations on the following page to help protect your personal information. INA also encourages you to enroll in the complementary services being offered to you through IDX by using the enrollment code provided above.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call IDX at 1-800-939-4170 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays). IDX call center representatives are fully versed on this incident and can answer any questions that you may have.

Please know that INA takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

John Sancenito

A handwritten signature in cursive script that reads "John J. Sancenito".

President
Information Network Associates

STEPS YOU CAN TAKE TO HELP PROTECT YOUR 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 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
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, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

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://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.