



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

June 28, 2024

**VIA ELECTRONIC MAIL**

Attorney General Anthony G. Brown  
Office of the Attorney General  
St. Paul Plaza  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202  
Telephone: 410-576-6491  
Email: [idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us)

**Re: Wold Architects and Engineers - Notice of Data Security Event**

To Attorney General Anthony G. Brown:

We represent Wold Architects and Engineers (“Wold”) located at 332 Minnesota St Ste W2000 Saint Paul, Minnesota 55101, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately two (2) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Wold 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 April 10, 2024, Wold discovered unusual activity in its digital environment. Upon discovering this activity, Wold immediately took steps to secure the network and launched an investigation, aided by cybersecurity specialists, to determine what happened and whether sensitive information may have been affected. As a result of the investigation, Wold learned that an unauthorized actor acquired certain files and data stored within its systems. Wold then launched a comprehensive review of these files to identify any personal information that may have been accessed. The review concluded on April 24, 2024 and Wold confirmed that personal information was included within the potentially accessed files.

The information that could have been subject to unauthorized access for Maryland residents includes first and last name, as well as driver’s license number, Social Security number, student or military identification, and passport number.

## **2. Notice to Maryland Residents**

On or about June 28, 2024, Wold provided written notice of this incident to two (2) Maryland residents. 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, Wold moved quickly to investigate and respond to the incident, assess the security of Wold systems, and identify potentially affected individuals. Wold is also working to implement additional safeguards and training to its employees. Wold 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, Wold is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Wold 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.

Wold is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

## **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.

Very truly yours,

A handwritten signature in cursive script that reads "Matthew Toldero".

Matthew Toldero of  
Constangy, Brooks, Smith & Prophete LLP

# **Exhibit A**



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

<<Date>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

## Notice of Data Security Incident

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

As you are aware, Wold Architects, Inc. ("Wold") recently experienced a security incident. We write this letter to provide further information about the incident, the type of information involved, and steps you can take to protect your information.

**What Happened?** On April 10, 2024, Wold discovered unusual activity in our digital environment. Upon discovering this activity, we immediately took steps to secure the network and launched an investigation, aided by cybersecurity specialists, to determine what happened and whether sensitive information may have been affected. As a result of the investigation, we learned that an unauthorized actor acquired certain files and data stored within our systems. We then launched a comprehensive review of these files to identify any personal information that may have been accessed. Our review concluded on April 24, 2024 and we confirmed that your personal information was included within the potentially accessed files.

**What Information Was Involved?** We determined that your name and <<Variable Data>> were included in the potentially accessed files.

**What Are We Doing?** As soon as we discovered this incident, we took measures to further secure the network and enlisted cybersecurity specialists to conduct a privileged forensic investigation. We have also implemented additional security measures to help reduce the risk of a similar incident occurring in the future. In addition, we are notifying you of this event and providing resources you can utilize to help protect your information.

Out of an abundance of caution, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: ## months of credit and CyberScan 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 free identity protection services by calling 1-800-939-4170, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00 a.m. – 9:00 p.m. Eastern Time. Please note the deadline to enroll is [DATE]. We also recommend that you review the guidance included with this letter about how to protect your information.

**For More Information.** If you have any questions about this letter, please call 1-800-939-4170, Monday through Friday from 9:00 a.m. – 9:00 p.m. Eastern Time.

The privacy and protection of personal information is a top priority for Wold. We deeply regret any inconvenience or concern this incident may cause.

Sincerely,  
Wold Architects, Inc.

## ADDITIONAL STEPS YOU CAN TAKE TO FURTHER 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). 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 Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.consumer.ftc.gov](http://www.consumer.ftc.gov), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).*

**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 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 this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, [www.equifax.com](http://www.equifax.com).*
- *Experian, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, [www.experian.com](http://www.experian.com).*
- *TransUnion, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, [www.transunion.com](http://www.transunion.com).*

**Fraud Alerts:** There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. 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>. Military members may also place an Active-Duty Military Fraud Alert on their credit reports while deployed. An Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

**Credit or Security Freezes:** Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the 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 via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

**IRS Identity Protection PIN:** You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

**You also have certain rights under the Fair Credit Reporting Act (FCRA):** These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit [http://files.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf).

**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.