



Alyssa Watzman, Partner
Cybersecurity & Data Privacy Team
1801 Broadway, Suite 520
Denver, CO 80202
AWatzman@constangy.com
Direct: 720.536.3234

November 5, 2024

VIA EMAIL

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

Re: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith, and Prophete LLP represents Diligent Delivery Systems (“Diligent”) in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in compliance with Maryland’s data breach notification statute.

1. Nature of the Security Incident

On July 11, 2024, Diligent became aware of unusual activity that disrupted access to certain of its systems. Upon discovering this activity, Diligent took steps to secure its digital environment and engaged leading, independent cybersecurity experts to assist with an investigation. As a result, Diligent learned that an unknown actor gained access to, and obtained, certain Diligent data. On or about October 25, 2024, Diligent learned that personal information was impacted in connection with this incident and worked to provide notification to potentially impacted individuals as quickly as possible.

2. Number of Affected Maryland Residents Notified

On November 5, 2024, Diligent notified fifty-nine (59) Maryland residents by letter mailed via first class U.S. mail. A sample copy of the notification letter is included with this correspondence.

The impacted information varied by individual, but may have included the residents’ Social Security number.

3. Measures Taken to Address the Incident

Upon discovering the incident, Diligent took the steps referenced above. Diligent also implemented additional security measures to further harden its environment in an effort to prevent a similar event from occurring in the future. Diligent also reported this incident to federal law enforcement and will cooperate with any investigation.

Diligent is also notifying the affected individuals and providing resources and steps individuals can take to help protect their information. The notification letter offers each individual complimentary credit monitoring and identity protection services through IDX by Zerofox. These services include 12 months of credit and CyberScan dark web monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. IDX will also support a call center to answer questions and assist with enrollment.

4. Contact Information

Diligent takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at AWatzman@constangy.com and David Rice at DR@constangy.com.

Best Regards,

/s/ Alyssa Watzman

Alyssa Watzman
CONSTANGY, BROOKS, SMITH &
PROPHETE LLP

Encl.: Sample Notification Letter



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

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

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

November 5, 2024

Re: Notice of <<Variable Text 2: Data Breach or Data Security Incident>>

Dear <<First Name>> <<Last Name>>:

I write to inform you of a recent data security incident experienced by Diligent Delivery Systems (“Diligent”) that may have affected your personal information. Diligent takes seriously the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information about the incident and steps that you can take to help protect your personal information.

What Happened? On July 11, 2024, Diligent became aware of unusual activity that disrupted access to certain of its systems. Upon discovering this activity, Diligent took steps to secure its digital environment and engaged leading, independent cybersecurity experts to assist with an investigation. As a result, Diligent learned that an unknown actor gained access to, and obtained, certain Diligent data. On or about October 25, 2024, Diligent learned that your personal information may have been impacted in connection with this incident. Notably, Diligent has no evidence that any personal information potentially impacted as a result of this incident has been misused.

What Information Was Involved? The potentially affected information included your name along with your <<Variable Text 1: Impacted Data>>.

What Are We Doing? Diligent value the data of its employees, customers, contractors, and vendors. As soon as Diligent discovered this incident, Diligent took the steps referenced above. Diligent also implemented additional security features to further bolster its security posture in an effort to reduce the risk of a similar incident to occur in the future and to further enhance its ability to preserve the confidentiality and integrity of all data in its possession. In addition, Diligent notified the Federal Bureau of Investigation and will provide whatever cooperation is necessary to hold the perpetrators of this incident accountable.

In this letter, Diligent is providing you with information about steps that you can take to help protect your personal information and is offering you complimentary identity protection services through IDX – a data incident and recovery services expert. These services include <<12/24 months>> months of credit¹ and dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services.

The deadline to enroll in these services is February 5, 2025. With this protection, IDX will help to resolve issues if your identity is compromised.

¹To 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. We encourage you to enroll in the complimentary credit monitoring and identity protection services we are offering. With this protection, IDX can help you resolve issues if your identity is compromised. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

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 1-866-398-3841 from 8:00 A.M. to 8:00 P.M. Central 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.

On behalf of Diligent, thank you for your understanding about this incident. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Very truly yours,

Diligent Delivery Systems

STEPS YOU CAN TAKE TO HELP PROTECT 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 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.

Internal Revenue Service Identity Protection PIN (IP PIN): You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification 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. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

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
<https://www.marylandattorneygeneral.gov/>
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

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>

1-401-274-4400

Washington D.C. Attorney General

441 4th 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://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>