



David McMillan, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street, Suite C-402
Brooklyn, New York 11201
dmcmillan@constangy.com
Direct: 718.614.8371

August 9, 2023

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents Slipstream Group, Inc, ("Slipstream") in connection with a recent data security incident described in greater detail below.

1. Nature of the security incident.

On March 21, 2023, Slipstream became aware of unusual activity in its computer network. In response, Slipstream took immediate steps to secure its digital environment and engaged a leading cybersecurity firm to conduct an investigation to determine whether any sensitive information may have been accessed or acquired during the incident. Based on the results of that investigation, Slipstream learned that an unauthorized actor gained access to certain files on its network. Following this confirmation, Slipstream engaged a vendor to conduct a comprehensive review of the potentially affected data and on July 10, 2023, Slipstream determined that personal information belonging to certain individuals may have been impacted in connection with this incident. Slipstream then worked diligently to obtain contact information to effectuate notification to potentially affected individuals.

Slipstream is notifying all potentially impacted individuals of this incident, providing them with steps they can take to protect their personal information, and offering them free credit and identity monitoring services. Slipstream has no evidence of any misuse or attempted misuse of any personal information in conjunction with this incident.

2. Number of Maine residents affected.

Slipstream notified two (2) Maine residents of this incident via first class U.S. mail on August 9, 2023. The information potentially impacted in connection with this incident includes name, and Social Security number. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as Slipstream discovered this incident, Slipstream took steps to secure its network environment and launched an investigation to determine what happened and the scope of personal information potentially impacted. In addition, Slipstream implemented measures to enhance the

August 9, 2023

Page 2

security of its environment in an effort to minimize the risk of a similar incident occurring in the future.

Slipstream has established a toll-free call center through IDX, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available at 1-888-939-4170 from 8:00 A.M. to 8:00 P.M. CST on Monday through Friday (excluding holidays). In addition, while Slipstream is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Slipstream is also providing complimentary credit and identity protection services to notified individuals.

4. Contact information.

Slipstream remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Constangy.

Best regards,

/s/ David McMillan

David McMillan
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter





Return to IDX:
4145 SW Watson Avenue, Suite 400
Beaverton, OR 97005

<< First Name >> << Last Name >>
<< Address 1 >> << Address 2 >>
<< City >>, << State >> << Zip >>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



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

August 9, 2023

Subject: Notice of Data <<Variable Text 1 – Breach or Security Incident>>

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

We are writing to notify you about a cybersecurity incident at Slipstream Group, Inc. (“Slipstream”) that may have affected your personal information. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened: On March 21, 2023, Slipstream became aware of unusual activity in its computer network. We immediately worked to investigate the activity with the assistance of our IT security provider, and engaged an outside cybersecurity firm to help contain the incident and conduct a forensic investigation. Based on the results of that investigation, we learned that an unauthorized actor gained access to our network between March 14, 2023 and March 25, 2023 and may have accessed or acquired certain files in the process. We then commenced a comprehensive review of the potentially affected data to determine whether any sensitive data was involved and whether individuals’ personal information may have been affected. That review concluded on July 10, 2023 and confirmed that your personal information was potentially impacted as a result of the incident which is the reason for this notification. Please note that Slipstream has no evidence of any actual or suspected misuse of this information.

What Information Was Involved? The information involved this incident may have included your name, as well as your <<Variable Text 2 – Data Elements>>.

What We Are Doing: As soon as we discovered this incident, we took steps to secure our environment and enlisted a leading, independent cybersecurity firm to conduct a forensic investigation. We also reported the incident to the FBI and have assisted in their investigation to hold the perpetrators accountable. In addition, we have implemented several technical measures in our environment to bolster Slipstream’s security posture and reduce chances of a similar incident occurring again.

While there is no evidence your information has been misused, out of an abundance of caution we are offering you complimentary credit monitoring and identity theft protection services through IDX – a data breach and recovery services expert. These services include: 24 months of credit¹ and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. To enroll, please call 1-800-939-4170, go to

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.

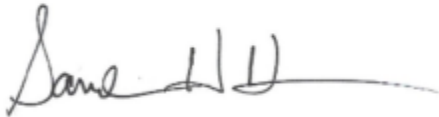
<https://app.idx.us/account-creation/protect>, or scan the QR image and using the Enrollment Code provided above. Please note that the deadline to enroll is November 9, 2023.

What You Can Do: We encourage you to enroll in the complimentary credit 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: If you have questions or need assistance, please contact 1-800-939-4170, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time, excluding major U.S. holidays. IDX representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Very truly yours,

A handwritten signature in black ink, appearing to read "Sandra Henry", with a long horizontal flourish extending to the right.

Sandra Henry, President and CEO
Slipstream Group, Inc.
431 Catalyst Way
Madison, WI 53719

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

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

Illinois Attorney General

Attorney General Kwame Raoul
100 W Randolph Street
Chicago, IL 60601
1-866-999-5630t

Wisconsin Attorney General

Attorney General Josh Kaul
Consumer Protection Division
P.O. Box 7857
Madison, WI 53707-7857
Fax: (608) 267-2779

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>