



Allen Sattler
650 Town Center Drive, Suite 1400
Costa Mesa, California 92626
Allen.Sattler@lewisbrisbois.com
Direct: 714.668.5572

March 10, 2022

VIA EMAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Bolton Global Capital, Inc. (“Bolton Global”) in connection with a data security incident described in greater detail below. This letter is to notify you of the incident on behalf of Bolton Global in accordance with Md. Code Ann. Comm. Law §§ 14-3501 - 3508.

I. Background

On September 8, 2021, Bolton Global discovered suspicious activity on its systems. Accordingly, Bolton Global took immediate steps to secure its digital environment and engaged independent cybersecurity experts to conduct a forensic investigation.

The forensic investigation determined that an unknown third-party gained access to Bolton Global’s network and may have acquired certain data without authorization. Following this finding, Bolton Global worked diligently to review the files that may have been accessed to identify the potentially impacted individuals and the categories of information involved for each.

II. Type of Information/Number of Residents Involved

On or about February 8, 2022, Bolton Global determined that the potentially impacted files contained some of Bolton Global’s customer information and that files with personal information relating to 48 Maryland residents may have been involved. The information involved included the following for these Maryland residents: name, Social Security number, Driver’s License number, passport number,

health information, and financial account number. Bolton Global has no evidence that any of this information has been misused.

III. Notification to Affected Individuals

On March 10, 2022, Bolton Global sent notification letters to potentially affected Maryland residents via USPS First Class Mail. Please find enclosed the sample notification letter. The notification letter provides information about the incident, the categories of personal information involved, and recommended steps that individuals may take to protect their information. It also offers complementary identity protection services by IDX, a global leader in risk mitigation and response. The services include credit monitoring, Cyberscan dark web monitoring, \$1 million identify theft reimbursement insurance, and fully managed identity recovery services for 12 months.

IV. Remediation Measures

Upon learning of this incident, Bolton Global implemented additional security measures to protect its network and systems to reduce the likelihood of future incidents. It will cooperate with the FBI and other law enforcement agencies to assist in identifying and prosecuting those responsible.

If you have any questions or need any additional information, please do not hesitate to contact me at 714.668.557 or Allen.Sattler@lewisbrisbois.com. Madaleine Gray is also available at 615.439.2701 and Madaleine.Gray@lewisbrisbois.com to address any follow up questions.

Sincerely,



Allen Sattler of
LEWIS BRISBOIS BISGAARD & SMITH LLP

AES:MJG

Encl: Sample Consumer Notification Letter
cc: Madaleine.Gray@lewisbrisbois.com

 **BOLTON**
GLOBAL CAPITAL
C/O IDX
P.O Box 989728
West Sacramento, CA 95798-9728



TO ENROLL, PLEASE CALL:
(833) 749-1699
OR VISIT:
<https://response.idx.us/bolton>
Enrollment Code: TV4JA9A3LE

Steven Roif
5073 Blackhawk Dr
Danville, CA 94506-4560



March 10, 2022

RE: Notice of Data Breach

Dear Steven Roif,

I am writing to inform you of a recent data security incident experienced by Bolton Global Capital, Inc. ("Bolton Global Capital") involving your personal information. Bolton Global Capital is an independent broker dealer offering wealth management services across all 50 U.S. states. Please read this letter carefully as it contains information about the incident, our response efforts, the type of information involved, and steps you can take to help protect your personal information.

What Happened: On September 8, 2021, Bolton Global discovered suspicious activity on its systems. In response, Bolton Global immediately began containment, mitigation, and restoration efforts to terminate the activity and to secure its network, systems, and data. In addition, Bolton Global retained independent cybersecurity experts to conduct a forensic investigation into the incident and to assist in determining what happened.

The forensic investigation revealed that an unknown third party had access to certain systems on Bolton Global's network from August 12, 2021 to September 9, 2021. Based on this finding, Bolton Global worked diligently to identify the potentially affected files and review the information contained in these files. On or about February 8, 2022, Bolton Global determined that the potentially impacted files contained some of Bolton Global's customer information. Please note that we have no indication that these files or the information contained in the files has been sold, published, shared, or otherwise misused as a result of this incident. Nevertheless, we wanted to notify you of the incident and provide resources to help protect your information.

What Information Was Involved: The data involved varies depending on the individual, but it may include the following information: Driver's License Number; Financial / Bank Account Number; Social Security Number (SSN). Again, we have no indication that this information has been sold, published, shared, or otherwise misused as a result of this incident.

What We Are Doing: Following the immediate steps described above, we implemented additional security measures to further harden our digital environment to minimize the likelihood of future incidents. We also reported the incident to the Federal Bureau of Investigation, and we are committed to providing whatever cooperation is necessary to help identify and prosecute those responsible.

In addition, we are offering you 12 months of complimentary identity theft protection services through IDX, a data breach and identity recovery services expert. The identity protection services include credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services at no cost to you. To receive these services, you must be over the age of 18 and have a Social Security number, an established credit file, and a residential address in the United States that is associated with your credit file.

What You Can Do: You can enroll in the complimentary identity protection services offered in this letter by calling **(833) 749-1699** or visiting <https://response.idx.us/bolton> and using the Enrollment Code provided at the top of this letter. Please note that the deadline to enroll is **June 10, 2022**. You can also review the enclosed sheet that provides additional steps you can take to help protect your information.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the identity protection services offered, please call (833) 749-1699, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time.

The privacy and security of your information is a top priority for Bolton Global Capital. We take this incident very seriously and we regret any worry or inconvenience this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Steve C. Preskenis".

Steve Preskenis, President
Bolton Global Capital, 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 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 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
www.consumer.ftc.gov and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

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

New York Attorney General

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

North Carolina Attorney General

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

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
www.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>.