



Richard Goldberg  
550 E. Swedesford Road, Suite 270  
Wayne, Pennsylvania 19087  
Richard.Goldberg @lewisbrisbois.com  
Direct: 215.977.4060

September 21, 2020

**VIA EMAIL**

Attorney General Gordon MacDonald  
Office of the Attorney General  
Consumer Protection Bureau  
33 Capitol Street  
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Stylex, a designer and manufacturer of seating and other furniture, based in Delanco, New Jersey. This letter is being sent on behalf of Stylex because the personal information of up two (2) New Hampshire residents may have been affected by a recent data security incident experienced by Stylex.

**1. Nature of the security incident.**

On August 1, 2020, Stylex discovered that they were the victim of a ransomware attack that encrypted the data stored on their servers. Stylex immediately initiated an investigation and took steps to secure its network and restore impacted data. Stylex also engaged cybersecurity experts to assist with the investigation and determine whether sensitive information may have been accessed during the incident. On or about September 4, 2020, the investigation revealed that personal information may have been accessed and/or acquired without authorization during the incident. The information that may have been accessed or taken includes current and former employees' or vendors' names, addresses, Social Security numbers and bank account information.

**2. Number of New Hampshire residents affected.**

A total of up to two (2) residents of New Hampshire may have been affected by this incident. Stylex will be notifying the potentially affected New Hampshire residents on or about September 21, 2020, via U.S. mail. A sample copy of the notification letter is being provided with this correspondence.

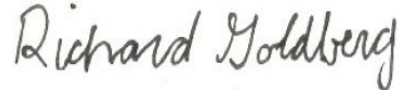
**3. Steps taken relating to the incident.**

Stylex implemented a more robust antivirus program, additional firewalls, reduced external access, and implemented additional auditing and tracking of external access. In addition, Stylex is offering twelve (12) months of complimentary credit and identity monitoring services to the potentially affected New Hampshire residents. Stylex has also notified the Federal Bureau of Investigation of this incident.

**4. Contact information.**

Stylex 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 me at (215) 977-4060 or by email at [Richard.Goldberg@lewisbrisbois.com](mailto:Richard.Goldberg@lewisbrisbois.com).

Sincerely,

A handwritten signature in black ink that reads "Richard Goldberg". The signature is written in a cursive, slightly slanted style.

Richard Goldberg  
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Consumer Notification Letter

**STYLEX**  
P.O. Box 5038  
Delanco, NJ 08075  
856.461.5600

<<FirstName>> <<LastName>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year)

To enroll, please visit:  
<https://app.myidcare.com/account-creation/protect>  
and enter  
Enrollment Code: \*\*\*\*

**Re: Notice of Data Breach**

Dear <<FirstName>> <<LastName>>,

I am writing to inform you about an incident that may have involved your personal information. The privacy and security of your information is extremely important to us. That is why I am writing to notify you of this incident, to offer you complimentary credit monitoring and identity protection services, and to inform you about steps that can be taken to help protect your personal information.

**What Happened?** On August 1, 2020, Stylex became aware of unusual activity in its network environment. An unauthorized person tried, but failed, to shut down our computer systems. Upon learning of the activity, Stylex took immediate steps to secure the network and launched an investigation of our systems. We also engaged a digital forensics firm to conduct an independent investigation to determine what happened and whether any employee, former employee, or vendor information was affected by the incident. On September 4, 2020 we learned that some of your personal information may have been accessed without authorization and may have been made public. We then notified you as soon as possible.

We have no evidence that your personal information has been misused. Nonetheless, out of an abundance of caution, we are writing to inform you of the incident and to provide you with access to complimentary credit monitoring and identity protection services.

**What Information Was Involved?** The following information may have been accessed without authorization: your name, Social Security number, and the number of the bank account where we deposited your compensation from Stylex.

**What We Are Doing.** As soon as Stylex discovered this incident we began an investigation. We are offering you one year of complimentary credit monitoring and identity protection services. This monitoring will be provided through IDExperts, a leading national identity protection firm. These services include:

**SINGLE BUREAU CREDIT MONITORING** - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

**CYBERSCANTM** - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

**IDENTITY THEFT INSURANCE** - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

**FULLY-MANAGED IDENTITY RECOVERY** - ID Experts' fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.

**What You Can Do.** We recommend that you activate your complimentary IDExperts services. To activate this service, call 1-800-939-4170 or go to <https://app.myidcare.com/account-creation/protect> and use the enrollment code at the top of this letter. You must activate these services by <<<date>>>. We also recommend that you review the guidance included with this letter about how to ensure your information is protected, in particular contacting your financial institution to ensure that your account is protected.

**For More Information.** If you have questions or need assistance, please contact our dedicated call center at <<Phone Number>>, Monday through Friday from <<Hours of Operation>>. IDExperts representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your personal information.

We take your trust in us and this matter very seriously. We regret any worry or inconvenience that this may cause you.

Sincerely,

Joe Kowalonek

CFO

[jkowalonek@stylexseating.com](mailto:jkowalonek@stylexseating.com)

## Steps You Can Take to Further Protect Your Information

**Notify Your Bank Account and Credit Card Companies:** If you received payments through direct deposit, your financial account information may have been compromised. You should call your bank, ask for the fraud department, and notify them of the potential for fraud and ask them to take effective measures to protect the funds in your account. You may want to do the same regarding your credit card accounts if those accounts were somehow connected to our system. Make sure you change online login credentials, passwords, and PINs.

**Notify the Tax Authorities:** You can call the IRS Identity Protection Specialized Unit at 800-908-4490 to advise them that your information may have been stolen. They will advise you on how to protect your tax filing information. You should also contact your state and local taxing authorities to do the same.

**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 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:

TransUnion	Experian	Equifax	Free Annual Report
P.O. Box 1000 Chester, PA 19016 1-800-909-8872 <a href="http://www.transunion.com">www.transunion.com</a>	P.O. Box 9532 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	P.O. Box 105851 Atlanta, GA 30348 1-800-685-1111 <a href="http://www.equifax.com">www.equifax.com</a>	P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 <a href="http://www.annualcreditreport.com">www.annualcreditreport.com</a>

**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 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. 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:** Under U.S. law, 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. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, [www.consumer.ftc.gov](http://www.consumer.ftc.gov) and [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General	Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
Bureau of Internet and Technology Resources 28 Liberty Street New York, NY 10005 <a href="mailto:ifraud@ag.ny.gov">ifraud@ag.ny.gov</a> 1-212-416-8433	200 St. Paul Place Baltimore, MD 21202 <a href="http://www.oag.state.md.us">www.oag.state.md.us</a> 1-888-743-0023	9001 Mail Service Center Raleigh, NC 27699 <a href="http://www.ncdoj.gov">www.ncdoj.gov</a> 1-877-566-7226	150 South Main Street Providence, RI 02903 <a href="http://www.riag.ri.gov">www.riag.ri.gov</a> 1-401-274-4400

**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 others. 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)