



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, CO 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

January 26, 2022

VIA EMAIL

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

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Stratis Visuals, LLC ("Stratis Visuals"), a printing company located in Torrington, Connecticut, in connection with a recent data security incident described in greater detail below. Stratis Visuals takes the protection of all information within its possession very seriously and has taken steps to help prevent similar incidents from occurring in the future.

1. Nature of the security incident.

On September 30, 2021, Stratis Visuals discovered that it had experienced an encryption event disrupting access to certain of its computer systems. In response, Stratis Visuals took immediate steps to contain the incident and to secure its digital environment. To that end, Stratis Visuals engaged an independent digital forensics firm to investigate the incident and to assist with its restoration efforts. Stratus Visuals has no evidence that any information has been misused. Nonetheless, out of an abundance of caution, Stratis Visuals has provided notification of this incident as well as identity theft protection services to individuals about whom it stored personal information including Social Security numbers, driver's license numbers, and financial information.

2. Number of Maryland residents affected.

Stratis Visuals sent notification letters to seventeen (17) residents of Maryland via first-class U.S. mail on January 26, 2022. A sample copy of the notification letter is attached hereto.

3. Steps taken relating to the incident.

Stratis Visuals has taken steps to help prevent similar incidents from occurring in the future. Those steps have included working with leading cybersecurity experts to enhance the security of its network and increasing its password complexity requirements. Stratis Visuals has also offered potentially affected individuals identity theft protection services monitoring at no cost through IDX, to ensure their information is protected.

4. Contact information.

Stratis Visuals remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (720) 292 - 2052 or via email at Alyssa.Watzman@lewisbrisbois.com.

Regards,

/s/ Alyssa R. Watzman

Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure(s): Sample Consumer Notification

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

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXX>>

January 26, 2022

Re: Notice of Data Security Incident

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

Stratis Visuals, LLC ("Stratis Visuals") is writing to inform you of an incident that may have involved your personal information. Stratis Visuals takes the privacy and security of all information very seriously. That is why I am writing to inform you of the incident and to advise you of certain steps that you can take to help protect your personal information.

What Happened? On September 30, 2021, Stratis Visuals discovered that it had experienced an encryption event disrupting access to certain of its computer systems. In response, Stratis Visuals took immediate steps to contain the incident and to secure its digital environment. To that end, Stratis Visuals engaged an independent digital forensics firm to investigate the incident and to assist with its restoration efforts. Stratis Visuals has no evidence that your personal information was impacted as a result of this incident but is providing notice of this incident to you because your personal information was stored on certain of the encrypted computer systems.

What Information Was Involved? The personal information belonging to you that was stored on certain of the encrypted computer systems included your name, <<Variable Text >>

What Are We Doing? As soon as Stratis Visuals discovered the incident, Stratis Visuals took the steps described above and implemented measures to enhance security in an effort to minimize the risk of a similar incident occurring in the future. In addition, although Stratis Visuals has no evidence of the misuse of any potentially impacted information, Stratis Visuals 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 breach and recovery services expert. These services include <<12 / 24>> months of credit¹ and dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Please note you must enroll by April 26, 2022.

What You Can Do: Please review the recommendations on the following page which describes steps you can take to help safeguard your information. Stratis Visuals also encourages you to activate the complimentary identity protection services being offered to you through IDX by using the enrollment code provided above.

For More Information: If you have questions or need assistance, please call IDX at 1-800-939-4170 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays).

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.

Protecting your information is important to us. Please know that we take this incident very seriously, and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Darci Vallez

Darci Vallez
CFO
Stratis Visuals

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

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>.

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

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

January 26, 2022

Re: Notice of Data Security Incident

Dear Parent or Guardian of <<First Name>> <<Last Name>>,

Stratis Visuals, LLC ("Stratis Visuals") is writing to inform you of an incident that may have involved your child's personal information. Stratis Visuals takes the privacy and security of all information very seriously. That is why I am writing to inform you of the incident and to advise you of certain steps that you can take to help protect your child's personal information.

What Happened? On September 30, 2021, Stratis Visuals discovered that it had experienced an encryption event disrupting access to certain of its computer systems. In response, Stratis Visuals took immediate steps to contain the incident and to secure its digital environment. To that end, Stratis Visuals engaged an independent digital forensics firm to investigate the incident and to assist with its restoration efforts. Stratis Visuals has no evidence that your child's personal information was impacted as a result of this incident but is providing notice of this incident to you because your child's personal information was stored on certain of the encrypted computer systems.

What Information Was Involved? The personal information belonging to your child that was stored on certain of the encrypted computer systems included your child's name and <<Variable Text >>

What Are We Doing? As soon as Stratis Visuals discovered the incident, Stratis Visuals took the steps described above and implemented measures to enhance security in an effort to minimize the risk of a similar incident occurring in the future. In addition, although Stratis Visuals has no evidence of the misuse of any potentially impacted information, Stratis Visuals is providing you with information about steps that you can take to help protect your child's personal information and is offering you complimentary identity protection services through IDX – a data breach and recovery services expert. These services include <<12/24>> months of dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Please note you must enroll by April 26, 2022.

What You Can Do: Please review the recommendations on the following page which describes steps you can take to help safeguard your child's information. Stratis Visuals also encourages you to activate the complimentary identity protection services being offered to you through IDX by using the enrollment code provided above.

For More Information: If you have questions or need assistance, please call IDX at 1-800-939-4170 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays).

Protecting your child's information is important to us. Please know that we take this incident very seriously, and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Darci Vallez

Darci Vallez
CFO
Stratis Visuals

Steps You Can Take to Protect Your Child's Information

Review Any Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review statements from your child's accounts 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 should also 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 (the "FTC").

Personal Information of a Minor: You can request that each of the three national consumer reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card, and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the consumer reporting agency. You can also report any misuse of a minor's information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <https://www.consumer.ftc.gov/articles/0040-child-identity-theft>. Contact information for the three national credit reporting agencies is below.

Security Freeze: You may place a free credit freeze for minors under age 16. By placing a security freeze, someone who fraudulently acquires the minor's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the 3 national credit reporting bureaus listed below to place the freeze. Keep in mind that when you place the freeze, the minor will not be able to borrow money, obtain instant credit, or get a new credit card until the freeze is temporarily lifted or permanently removed. You must separately place a security freeze on the minor's credit file with each credit reporting agency. There is no charge to place, lift, or remove a security freeze on the minor's credit files. In order to place a security freeze, you may be required to provide the credit reporting agency with information that identifies you and/or the minor, including birth or adoption certificate, Social Security card, and government issued identification card.

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 the minor's credit report. An initial fraud alert is free and will stay on the minor's credit file for at least one year. The alert informs creditors of possible fraudulent activity within the minor's report and requests that the creditor contact you prior to establishing any accounts in the minor's name. To place a fraud alert on the minor's credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

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

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001

ncdoj.gov
1-877-566-7226

http://www.riag.ri.gov
1-401-274-4400

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 the minor's 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>.