LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Maria Efaplomatidis
77 Water Street, Suite 2100
New York, New York 10005
Maria.Efaplomatidis@lewisbrisbois.com
Direct: 212.232.1366

November 21, 2022

File No. 39395.606

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330
Email: breach.security@maine.gov

Re: **Notification of Data Security Incident**

Dear Attorney General Aaron Frey:

Lewis Brisbois Bisgaard & Smith LLP represents South Walton Fire District ("SWFD") in connection with a ransomware incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maine's data breach notification statute. (Me. Rev. Stat. Tit. 10 §§ 1346 – 1350-B).

1. Nature of the Security Incident

On May 30, 2022, SWFD learned that an unauthorized actor temporarily gained access to its computer network and encrypted certain systems. In response, SWFD took immediate steps to secure its environment and promptly launched an investigation. SWFD engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On October 20, 2022, SWFD learned that personal information ("PI"), to include protected health information ("PHI"), belonging to certain individuals may have been impacted in connection with the incident. While there is no evidence of the misuse of any of data, SWFD has proactively taken steps to effectuate notification to all potentially impacted individuals.

2. Number of Maine Residents Involved

SWFD notified 11 Maine residents of this incident via First-Class U.S. Mail on November 21, 2022. A sample copy of the notification letter is also included with this correspondence. *See* enclosure. The PI and PHI involved differ depending on the individual but may include name, address, date of birth, Social Security number, and medical and health insurance related information.

3. Steps Taken Relating to the Incident

As soon as SWFD discovered this incident, SWFD took steps to secure its systems and launched an investigation to determine what happened and whether personal information had been accessed or acquired without authorization. SWFD has also implemented additional safeguards to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future.

SWFD has also 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. While SWFD is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, SWFD is also providing complimentary identity protection services to notified individuals for a period of 12 months. These services include credit and dark web monitoring, identity restoration, and a $1 million identity fraud loss reimbursement.

4. Contact Information

SWFD is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Maria Efaplomatidis at Maria.Efaplomatidis@lewisbrisbois.com or 212.232.1366.

Sincerely,

Maria Efaplomatidis of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

Encl.: Sample Consumer Letter

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

To Enroll, Please Call:
1-833-814-1731
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment Code>>

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

November 21, 2022

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

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

I am writing to inform you of a ransomware incident experienced by South Walton Fire District ("SWFD") that may have affected your personal information. SWFD takes the privacy and security of all personal information, including protected health information, within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened? On May 30, 2022, we learned that an unauthorized actor temporarily gained access to our computer network. We took immediate action to secure our environment and notified federal, state, and local law enforcement authorities. In response, we engaged independent digital forensics and incident response experts to determine what happened and to identify any data that may have been accessed or acquired without authorization as a result.

On October 20, 2022, we learned that your personal information may have been impacted in connection with this incident. Please note that we have no evidence of the misuse or attempted misuse of any potentially impacted information. However, out of an abundance of caution, SWFD has worked to identify all potentially affected individuals in order to provide notice of the incident and resources to help with credit and identity protection.

What Information Was Involved? The information potentially impacted in connection with this incident included your <<Variable Text 2: Potentially Impacted Data Sets>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. In addition, we implemented measures to enhance the security of our environment in an effort to minimize the risk of a similar incident occurring in the future. We also reported the incident to law enforcement and are cooperating with the FBI to aid in their investigation.

Although we have no evidence of the misuse of any potentially impacted information, we are providing you with information about steps that you can take to help protect your personal information and offering you complimentary credit and identity protection services through IDX – a data breach and recovery services expert. These services include <<12/24>> months of credit[1] 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 21, 2023. With this protection, IDX will help to resolve issues if your identity is compromised.

[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.

What You Can Do: Please review this letter carefully along with the "Steps You Can Take to Help Protect Your Information" document enclosed with this letter. It describes additional ways you can help safeguard your information. Specifically, we also recommend that you review your credit and/or identity report for unusual activity, as well as any explanation of benefits (EOBs) or medical bills received to ensure the charges are for services you received. If you see anything that you do not understand or that looks suspicious, you should contact your state Attorney General's Office or the consumer reporting agencies for assistance using the contact information included in this letter.

For More Information: If you have questions or need assistance, please call IDX at 1-833-814-1731 from 8:00 A.M. to 8:00 P.M. Central Time, Monday through Friday (excluding holidays). Representatives are fully versed on this incident and can answer any questions that you may have.

The security of your information is a top priority at SWFD, and protecting patient information at all costs is a critical operational piece to SWFD's role as a care provider. Please accept my sincere apologies and know that we take this matter very seriously and deeply regret any worry or inconvenience this may cause you.

Sincerely,

Ryan H. Crawford
Fire Chief / Administrator
South Walton Fire District
911 N County Hwy 393
Santa Rosa Beach, FL 32459

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
1-877-438-4338

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

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.

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

To Enroll, Please Call:
1-833-814-1731
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<Enrollment Code>>

To the Parent or Guardian of:
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

November 21, 2022

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

To the Parent(s) or Guardian of <<First Name>> <<Last Name>>,

I am writing to inform you of a ransomware incident experienced by South Walton Fire District ("SWFD") that may have affected your child's personal information. SWFD takes the privacy and security of all personal information, including protected health information, within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your child's personal information.

What Happened? On May 30, 2022, we learned that an unauthorized actor temporarily gained access to our computer network. We took immediate action to secure our environment and notified federal, state, and local law enforcement authorities. In response, we engaged independent digital forensics and incident response experts to determine what happened and to identify any data that may have been accessed or acquired without authorization as a result.

On October 20, 2022, we learned that your child's personal information may have been impacted in connection with this incident. Please note that we have no reason to believe that your child's personal information has been published, shared, or misused. However, out of an abundance of caution, SWFD has worked to identify all potentially affected individuals to provide notice of the incident and resources to help with identity protection.

What Information Was Involved? The information potentially impacted in connection with this incident included your child's <<Variable Text 2: Potentially Impacted Data Sets>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. In addition, we implemented measures to enhance the security of our environment in an effort to minimize the risk of a similar incident occurring in the future. We also reported the incident to law enforcement and are cooperating with the FBI to aid in their investigation.

To help relieve concerns and restore confidence following this incident, we have secured the services of IDX to provide identity theft protection services for your child at no cost to you for <<12/24>> months. IDX is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. The identity monitoring services include dark web monitoring, $1 million in identity theft expense reimbursement insurance, and fully managed identity recovery services. With this protection, IDX will help to resolve issues if your child's identity is compromised.

Visit https://app.idx.us/account-creation/protect to activate the identity monitoring services.
Enrollment Code: <<Enrollment Code>>.
The deadline to enroll in these services is February 21, 2023.

What You Can Do: We encourage you to activate the identity monitoring services we are making available through IDX. Please also review the enclosed "Steps You Can Take to Protect Your Child's Information" included with this letter. It describes additional steps you can take to help protect your child, including recommendations regarding identity theft protection.

For More Information: If you have questions or need assistance, please call IDX at 1-833-814-1731 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.

The security of your child's information is a top priority at SWFD, and protecting patient information at all costs is a critical operational piece to SWFD's role as a care provider. Please know that we take this matter very seriously and deeply regret any worry or inconvenience this may cause you.

Sincerely,

Ryan H. Crawford
Fire Chief / Administrator
South Walton Fire District
911 N County Hwy 393
Santa Rosa Beach, FL 32459

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 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-800-831-5614
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. This 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, 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
1-877-438-4338

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

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
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
400 S 6th 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 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://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.