



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Josh Brian
Office: (267) 930-2405
Fax: (267) 930-4771
Email: JBrian@mullen.law

3001 N. Rocky Point Drive East, Suite 200
Tampa, FL 33607

November 30, 2022

VIA E-MAIL

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

Re: Supplemental Notice of Data Event

To Whom It May Concern:

We represent Sigmund Software, LLC (“SSL”) located at 83 Wooster Heights Road, Suite 350, Danbury, CT 06810, and write to notify your office of an event that may affect certain information relating to approximately one (1) Maryland resident. The investigation into this matter is ongoing, and this notice may be supplemented if any material facts are learned subsequent to its submission. By providing this notice, SSL does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction. Please note, SSL first started providing notice to your office on October 20, 2022, and November 14, 2022.

Nature of the Data Event

SSL provides electronic health record management services to health care providers. Accordingly, SSL received certain patient data in connection with these services. On September 9, 2022, SSL identified unusual activity on its computer network. In response, SSL began an investigation to determine the nature and scope of the activity. This investigation is ongoing; however, on September 22, 2022, SSL learned that certain files were downloaded without authorization. SSL notified the health care provider and these files were reviewed for potentially sensitive information. SSL and the health care provider diligently worked to determine contact details for those individuals whose information was in the files, which concluded on October 19, 2022. The following categories of information were identified in the reviewed files: name and Medical Record number, CPT Code, and healthcare cost.

Notice to Maryland Resident

On or about November 30, 2022, SSL continued providing written notice of this event to approximately one (1) Maryland resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon identifying the event, SSL began an investigation to assess the scope of the event, the security of SSL systems, and identify potentially affected individuals. Further, SSL notified federal law enforcement regarding the event. SSL is evaluating additional safeguards to mitigate risk of reoccurrence. SSL is providing access to credit monitoring services for one (1) year, through Experian, to individuals whose information was potentially affected by this event, at no cost to these individuals.

Additionally, SSL is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud. SSL is providing the individuals with information on how to place a fraud alert and credit freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

SSL is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data event, please contact us at (267) 930-2405.

Very truly yours,

Josh Brian of
MULLEN COUGHLIN LLC

JPB/cob
Enclosure

EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

November 30, 2022

i6641-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 ADULT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



[Extra1]

Dear Sample A. Sample:

Sigmund Software, LLC (“SSL”) provides electronic health record management services to health care providers and received your information in connection with these services. SSL writes to inform you of an event that involved some of your information. SSL is providing information about the event, SSL’s response, and steps you may take, should you feel it is appropriate to do so.

What Happened? On or about September 9, 2022, SSL experienced unusual activity on its computer network. In response, SSL began an investigation to determine the nature and scope of the activity. This investigation is ongoing; however, on September 22, 2022, SSL learned that certain files were downloaded without authorization. These files were reviewed for potentially sensitive information, and SSL diligently worked to determine contact details for those individuals whose information was in the files, which concluded on October 19, 2022.

What Information Was Involved? Although SSL has no evidence that any sensitive information has been misused by third parties as a result of this event, we are notifying you for purposes of full transparency.

Based on the investigation, the following information was identified in the reviewed [Extra2] files: your name, [Extra3]. The reviewed files **did not** include your email address, phone number, diagnosis, prescriber/therapist/group notes, social security number, credit card information or passwords.

What SSL is Doing. SSL takes this event and the security of information in its care seriously. As part of SSL’s ongoing commitment to the privacy of information in its care, SSL is evaluating additional technical security measures, and existing policies and procedures to mitigate reoccurrence of this type of event. Further, SSL is offering complimentary identity monitoring services to you.

What You Can Do. SSL encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and free credit reports for suspicious activity and to detect errors. SSL also recommends you review the “Steps You Can Take to Protect Personal Information” section of this letter. Further, you may enroll in the offered complimentary credit monitoring and identity protection services. Enrollment instructions for the complimentary monitoring services are in the next section of this letter.

For More Information. If you have additional questions, please contact SSL’s dedicated assistance line at (888) 397-0071, Monday through Friday from 9:00 a.m. to 11:00 p.m. and Saturday and Sunday from 11:00 a.m. to 8:00 p.m. Eastern Time (excluding U.S. holidays). You may also write to SSL at Sigmund Software, 83 Wooster Heights Road, Suite 350, Danbury, CT 06810.

Sincerely,

Sigmund Software, LLC

0000001



i6641-L01

ENGAGE#

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, SSL is offering a complimentary [Extra4]-month membership of Experian's IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: February 28, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (888) 397-0071 by February 28, 2023. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the identity restoration services by Experian.

Additional Details Regarding Your [Extra4]-Month Experian Identityworks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 397-0071. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for [Extra4] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will

0000001



likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For Massachusetts Residents, under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. SSL encourages you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.