



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Matthew V. Toldero
Office: (267) 930-4554
Fax: (267) 930-4771
Email: mtoldero@mullen.law

19109 West Catawba Avenue, Suite 200
Cornelius, NC 28031

September 28, 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: Notice of Data Event

Dear Sir or Madam:

We represent Sandler Systems, LLC (“Sandler”), located at 300 Red Brook Boulevard, Suite 400, Owings Mills, MD 21117, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Sandler 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.

Nature of the Data Event

On or about May 11, 2022, Sandler became aware of unusual activity related to an employee’s email account. Sandler immediately began an investigation, with the help of forensic investigation specialists, to better understand the nature and scope of this activity. On July 15, 2022, it was determined that the certain Sandler employee email accounts were accessed without authorization for a limited amount of time. It was not possible to determine exactly which email messages or attachments may have been accessed or viewed without authorization. In an abundance of caution, a detailed and thorough review of the contents of the email account was performed to determine whether sensitive information was contained in any of the email messages or attachments within this employee’s account. Upon receiving the results of the detailed review of the email contents on August 26, 2022, Sandler worked diligently to provide any potentially affected individuals notice.

The information that could have been subject to unauthorized access includes name, and medical treatment information.

Notice to Maryland Resident

On September 28, 2022, Sandler provided written notice of this incident to 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 discovering the event, Sandler moved quickly to investigate and respond to the incident, assess the security of Sandler systems, and identify potentially affected individuals. Sandler is also working to implement additional safeguards and training to its employees.

Additionally, Sandler is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Sandler is providing individuals with information on how to place a fraud alert and security 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.

Sandler 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 security event, please contact us at (267) 930-4554.

Very truly yours,

Matthew V. Toldero of
MULLEN COUGHLIN LLC

MVT/rmm
Enclosure

EXHIBIT A

<<Return Mail Address>>

<<Name>>

<<Address1>>

<<Address 2>>

<<Date>>

<<City, State, ZIP>>

NOTICE OF SECURITY INCIDENT

Dear <<Name>>:

As you are aware, Sandler Systems LLC (“Sandler”) recently experienced an event that may impact the security of some of your information. Although we have received no indication of any actual or attempted misuse of your information as a result of this event, this notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is necessary to do so.

What Happened? On or about May 11, 2022, Sandler became aware of unusual activity related to an employee’s email account. We immediately began an investigation, with the help of forensic investigation specialists, to better understand the nature and scope of this activity. On July 15, 2022, it was determined that the certain Sandler employee email accounts were accessed without authorization for a limited amount of time. It was not possible to determine exactly which email messages or attachments may have been accessed or viewed without authorization. In an abundance of caution, a detailed and thorough review of the contents of the email account was performed to determine whether sensitive information was contained in any of the email messages or attachments within this employee’s account. Upon receiving the results of the detailed review of the email contents on August 26, 2022, we worked diligently provide you notice.

What Information Was Involved? The investigation determined that your name, address, and <<Data Elements>> may have been accessible.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon learning of the event, we moved quickly to investigate and respond to the event, assess the security of our systems, and notify potentially affected individuals. In order to mitigate harm and protect against further incidences, a leading cybersecurity forensics firm worked with internal teams to thoroughly investigate and ensure the security of the email environment. Employee user accounts passwords were reset, and multifactor authentication is being implemented.

We are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity and to report any suspicious activity promptly to your bank or financial institution. Additional information and resources are included in the enclosed *Steps You Can Take To Protect Personal Information*.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please contact us at XXX-XXX-XXXX, Monday through Friday from [TIMES], or Saturday through Sunday from [TIMES]. Again, we take the privacy and security of information in our care very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,
Sandler Systems LLC

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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 one 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 security freeze, you will need to provide 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, 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, DC 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 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 www.oag.state.md.us. Sandler Systems LLC is located at 300 Red Brook Boulevard, Suite 400, Owings Mills, MD 21117.