



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Lynda Jensen
Office: (267) 930-2303
Fax: (267) 930-4771
Email: Ljensen@mullen.law

3 Allied Drive, Suite 303
Dedham, MA 02026

February 21, 2023

VIA E-MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent S&K Manufacturing, Inc. ("S&K") located at 1001 Liberty Industrial Drive, O'Fallon, MO 63366, and are writing to notify your office of an event that may affect the security of certain personal information relating to one hundred (100) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, S&K 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 March 1, 2022, S&K's third-party Managed Service Provider, Freestyle Solutions ("Freestyle"), informed S&K that it discovered suspicious activity on one of its servers, which hosted customer payment card information. To determine the nature and scope of the activity, and to ensure the integrity of its systems, Freestyle launched an investigation with the assistance of cybersecurity specialists. S&K understands that the investigation confirmed an unknown actor accessed the environment between September 18, 2020 and February 3, 2022, and, during that period, installed malware and potentially acquired or viewed customer payment card information maintained. On May 5, 2022, S&K received information from Freestyle identifying a population of individuals whose information was potentially accessed. S&K then launched its own investigation to understand the event and its potential impact on the identified individuals. S&K also worked to identify current addresses for those identified individuals. Although S&K has no

indication of any misuse of personal information as a result of this event, out of an abundance of caution, S&K is providing notice to individuals who may have been impacted.

The information that could have been subject to unauthorized access includes name and payment card information.

Notice to Maryland Residents

On or about February 21, 2023, S&K provided written notice of this event to one hundred (100) Maryland residents. 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 and its potential impact on individuals, S&K moved to investigate and respond to the event and identify potentially affected individuals.

Additionally, S&K is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. S&K is providing individuals with information on how to place fraud alerts and credit freezes on their credit files, 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.

S&K is providing written notice of this event to relevant state regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the event, please contact us at (267) 930-2303.

Very truly yours,

Lynda Jensen of
MULLEN COUGHLIN LLC

LRJ/lhw
Enclosure

EXHIBIT A

S&K Manufacturing
c/o Cyberscout
P.O. Box 3923
Syracuse, NY 13220



1001 Liberty Industrial Dr.
O'Fallon, MO 63366

February 21, 2023

NOTICE OF DATA BREACH

Dear:

S&K Manufacturing, Inc. ("S&K") is providing notice of a data event that may impact the privacy of certain individuals' personal information. We are providing information about the event and our response. We are unaware of any identity theft or fraud resulting from this event. We are providing this notice out of an abundance of caution.

What Happened? On March 1, 2022, our third-party Managed Service Provider, Freestyle Solutions ("Freestyle"), informed us that it discovered suspicious activity on one of its servers, which hosted customer payment card information. To determine the nature and scope of the activity, and to ensure the integrity of its systems, Freestyle launched an investigation with the assistance of cybersecurity specialists. We understand that the investigation confirmed an unknown actor accessed the environment between September 18, 2020 and February 3, 2022, and, during that period, installed malware and potentially acquired or viewed customer payment card information maintained. On May 5, 2022, we received information from Freestyle identifying a population of individuals whose information was potentially accessed. We then launched our own investigation to understand the event and its potential impact on the identified individuals. Although we have no indication of any misuse of your personal information as a result of this event, out of an abundance of caution, we are providing notice to individuals who may have been impacted.

What Information Was Involved? The following information relating to you was present in data stored on Freestyle's server during the period of unauthorized access: name and payment card information. We do not have information at this time whether the present payment card information was valid or expired at the time of potential unauthorized access. Please note, we have no evidence of any actual or attempted misuse of personal information as a result of the event.

What We Are Doing. We take this event and the security of personal information very seriously. In response to the event, Freestyle reports that it removed the malware within the environment and launched an investigation, aided by cybersecurity specialists, to confirm the nature and scope of the event. Further, as part of our ongoing commitment to the privacy of information in our care, we have coordinated with the Freestyle team to understand the steps it has taken and will continue to take to protect information that it holds. We have also decided to end our relationship with Freestyle and engage a new managed service provider.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and by monitoring your free credit reports for suspicious activity and to detect errors. You can find out more about how to protect against the potential misuse of information in the enclosed *Steps You Can Take to Protect Information*. There, you will also find more information about the identity monitoring services we are offering and how to enroll.

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 call 833-570-2917, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding U.S. holidays. You may also write to us at: 1001 Liberty Industrial Drive, O'Fallon, MO 63366.

We apologize for any inconvenience this event may cause you.

Sincerely,

S&K Manufacturing, Inc.

STEPS YOU CAN TAKE TO PROTECT INFORMATION

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 one-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 credit 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 fraud alert or 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	1-800-916-8800
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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

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.

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 violator. 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. We encourage 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/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event. There are 3 Rhode Island residents impacted by this event.