



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 21, 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 Flaghouse, Inc. ("Flaghouse") located at 601 FlagHouse Drive, Hasbrouck Heights, NJ 07604 and are writing to notify your office of an incident that may affect the security of some 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, Flaghouse 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 February 13, 2021, Flaghouse became aware that certain systems within its network were not working. Flaghouse began working with its internal IT and determined that certain records may have been encrypted. Flaghouse immediately launched an investigation with the assistance of third-party forensic specialists to confirm the full nature and scope of the incident and restore functionality of impacted systems. The Flaghouse team was able to quickly secure the Flaghouse systems and restore impacted files. Further investigation revealed that a limited amount of information may have been accessed without authorization during this event. Flaghouse immediately began to review the information that may have been subject to access. However, due to the scope of the review, on April 7, 2021, Flaghouse determined that it required third party review specialists to assist with a comprehensive review of all potentially impacted files. On December 15, 2021, Flaghouse, with the assistance of third-party specialists, completed the

comprehensive review and determined that information associated with one (1) Maryland resident may have been accessible during this event.

The information that could have been subject to unauthorized access may include name and Social Security number.

Notice to Maryland Resident

On or about January 21, 2022, Flaghouse began provided written notice of this incident to affected individuals, which includes 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, Flaghouse moved quickly to investigate and respond to the incident, assess the security of Flaghouse systems, and notify potentially affected individuals. Flaghouse is also working to implement additional safeguards and training to its employees. Flaghouse is providing access to credit monitoring services for one (1) year, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Flaghouse is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Flaghouse 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/bo1
Enclosure

EXHIBIT A



Enriching lives. Delivering solutions.™

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(SubjectLine)>>

Dear <<first_name>>:

Flaghouse, Inc. ("Flaghouse") writes to inform you of an incident that may affect the security of some of your personal information. This notice provides information about the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? On or around February 13, 2021, Flaghouse became aware that certain systems within its network were not working. We began working with our IT department and determined that certain records may have been encrypted. We immediately launched an investigation with the assistance of third-party forensic specialists to confirm the full nature and scope of the incident and restore functionality of impacted systems. We were able to secure the Flaghouse systems and restore impacted files. Further investigation revealed that certain information may have been accessed without authorization during this event. We immediately began to review the information that may have been subject to access. However, due to the scope of the review, Flaghouse required third-party review specialists to assist with a comprehensive review of all potentially impacted files. On December 15, 2021, we completed this review and determined that information associated with certain individuals, including you, was contained in the impacted files at the time of the incident.

What Information Was Involved? The information related to you and maintained by Flaghouse that may have been accessed included your <<b2b_text_2(DataElements)>>.

What We Are Doing. We take the security of information entrusted to us very seriously and apologize for any inconvenience this incident may cause. As part of our ongoing commitment to the security of information within our care, we have performed a review of our existing policies and procedures regarding cybersecurity, have already implemented a number of improvements to strengthen our security and will continue to evaluate additional measures and safeguards to protect against this type of incident in the future.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account and monitoring credit reports for suspicious activity and to detect errors. You may also review the information contained in the attached *Steps You Can Take to Help Protect Personal Information*. Although we are not aware of any actual or attempted misuse of your personal information, as an added precaution we have arranged to offer you access to 12 months of complimentary credit monitoring services provided through Kroll. Although we are making these services available to you, we are unable to activate you directly. For activation instructions, please review the information contained in the attached *Steps You Can Take to Help Protect Personal Information*.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please contact our dedicated assistance line at 1-???-???-???, Monday through Friday, during the hours of 9:00 a.m. – 6:30 p.m. Eastern Time.

Sincerely,

George Carmel
President

Steps You Can Take to Help Protect Personal Information

Activate Complimentary Credit Monitoring



Your monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until **<<b2b_text_6(EnrollmentDeadline)>>** to activate your identity monitoring services.

Membership Number: **<<MembershipNumber(S_N)>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit 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.

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 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
888-298-0045	1-888-397-3742	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.

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.