



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

AUG 30 2021

CONSUMER PROTECTION

Alexandria N. Murphy
Office: (267) 930-1345
Fax: (267) 930-4771
Email: amurphy@mullen.law

40 Burton Hills Boulevard, Suite 200
Nashville, TN 37215

August 24, 2021

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Syufy Enterprises, LP (“Syufy”), located at 150 Pelican Way, San Rafael, CA 94901, and are writing to notify your office of an incident that may affect the security of some personal information relating to three (3) New Hampshire residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Syufy does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On September 16, 2020, Syufy detected suspicious activity on certain systems on its network. Syufy immediately launched an investigation to determine the nature and scope of the incident. Through the investigation, Syufy identified certain files and folders on the network that may have been viewed or taken by an unauthorized actor between September 7, 2020 and September 15, 2020. Although the investigation could not definitively confirm whether an unauthorized actor viewed or took such files, in an abundance of caution, Syufy conducted a thorough review of the potentially impacted files to determine whether they contained any sensitive information. This review was completed on or about March 1, 2021. Syufy thereafter worked to identify address information in order to notify potentially impacted individuals.

The information that could have been subject to unauthorized access includes name, address, and financial account information.

Mullen.law

Notice to New Hampshire Residents

On or about August 24, 2021, Syufy provided written notice of this incident to all potentially affected individuals, which includes three (3) New Hampshire 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, Syufy moved quickly to investigate and respond to the incident, assess the security of Syufy systems, and notify potentially affected individuals. Syufy is also working to implement additional safeguards and training to its employees.

Additionally, Syufy is providing potentially 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. Syufy 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) 930-1345.

Very truly yours,



Alexandria N. Murphy of
MULLEN COUGHLIN LLC

ANM/acl
Enclosure

EXHIBIT A

SYUFY ENTERPRISES

P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

August 24, 2021

Re: Notice of Data <<Event/Breach>>

Dear <<First Name>> <<Last Name>>:

Syufy Enterprises, LP (“Syufy”) is committed to protecting the privacy and security of the information entrusted to us. We are writing to inform you of a recent event that may impact some of your information. Although we are unaware of any actual or attempted misuse of your information, we are providing you with details about the event, steps we are taking in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? On September 16, 2020, we detected suspicious activity on certain systems on the Syufy network. We immediately launched an investigation to determine the nature and scope of the incident. Through the investigation, we identified certain files and folders on the network that may have been viewed or taken by an unauthorized actor between September 7, 2020 and September 15, 2020. Although the investigation could not definitively confirm whether an unauthorized actor viewed or took such files, in an abundance of caution, we conducted a thorough review of the potentially impacted files to determine whether they contained any sensitive information. This review was completed on or about March 1, 2021. We thereafter worked to identify address information in order to notify potentially impacted individuals, which we have now completed.

What Information Was Involved? We cannot confirm if the unauthorized actor(s) viewed or took any specific information relating to you. However, we determined that the potentially at-risk files contained your name, <<data elements>>.

What We Are Doing. We took steps to contain the incident, including resetting user passwords promptly upon discovery. As part of our ongoing commitment to the privacy and security of information in our care, we are evaluating opportunities to improve security and to better prevent future events of this kind.

What You Can Do. As a precaution, 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 better protect against the potential misuse of information in the enclosed *Steps You Can Take to Protect Your 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, we encourage you to call our dedicated assistance line at 1-833-909-3940, which is available Monday through Friday, from 6:00 a.m. to 6:00 p.m., Pacific Time. You may also write to us at: 150 Pelican Way, San Rafael, CA 94901.

We apologize for any inconvenience this incident may cause you and remain committed to the privacy and security of information in our possession.

Sincerely,

A handwritten signature in black ink, appearing to read "Andrew", written over a thin vertical line.

Andrew Cuyugan McCullough
Executive Vice President, Business Affairs

STEPS YOU CAN TAKE TO PROTECT YOUR 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, military identification, 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 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW, Washington, D.C. 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. Syufy is located at 150 Pelican Way, San Rafael, CA 94901.

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; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.

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/>.