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

October 21, 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 SCUF Gaming International, LLC ("SCUF Gaming") located at 3970 Johns Creek Court, Suite 325, Suwanee, GA 30024 and are writing to notify your office of an incident that may affect the security of some personal information relating to one hundred fifty (150) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, SCUF Gaming 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 February 18, 2021 SCUF Gaming received notice from its payment processor of unusual activity on credit cards used at its online store. SCUF Gaming conducted a rigorous investigation in partnership with third-party forensic specialists and on March 16, 2021 an unauthorized script was detected and immediately removed. Through further investigation, the third-party forensic specialists were able to identify what the script could do and determined on April 21, 2021 that the script was capable of capturing credit card information. SCUF Gaming then worked to determine the window of time where credit card information could have potentially been exposed which concluded on July 21, 2021. The investigation confirmed that there was a chance the unauthorized script present on SCUF Gaming's site may have exposed personal information at point of sale for purchases between February 3, 2021 and removal of the script on March 16, 2021. SCUF Gaming was unable to confirm if any credit card transactions during this time period were affected. While

its investigation was ongoing, SCUF Gaming sent an email to potentially affected individuals on May 4, 2021 with details pertaining to the incident and SCUF Gaming's response. The information that could have been subject to unauthorized access includes cardholder name, email address, billing address, credit card number, expiration date, and CVV.

Notice to New Hampshire Residents

On or about October 21, 2021, SCUF Gaming provided written notice of this incident to affected individuals, which includes one hundred fifty (150) 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

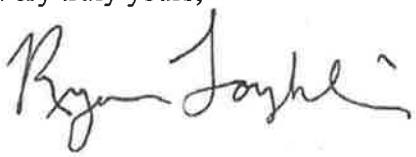
Upon discovering the event, SCUF Gaming moved quickly to investigate and respond to the incident, assess the security of SCUF Gaming systems, and notify potentially affected individuals. SCUF Gaming is also working to improve upon its security protocols, enhance its security features, and increase the scrutiny of its third-party vendors.

Additionally, SCUF Gaming 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. SCUF Gaming 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/jcj

EXHIBIT A

SCUF GAMING

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

<<VARIABLE HEADER>>

Dear <<Name 1>>:

As a follow-up to our email sent on May 4, 2021, SCUF Gaming International, LLC ("SCUF Gaming") is contacting you again now that the investigation is complete to inform you of a security incident that may have compromised the payment card you used in March 2021 for a transaction or attempted transaction at www.scufgaming.com. This communication does not mean that fraud did or will occur on your payment card account. You should monitor your account and notify your card provider of any unusual or suspicious activity. As a precaution, you may wish to request a new payment card number from your provider.

What Happened? On February 3, 2021, login credentials for a third-party vendor were used to insert an unauthorized script onto the backend system of SCUF Gaming's webstore. The unauthorized script was detected on March 16, 2021 and removed immediately on that same day. We conducted a rigorous investigation in partnership with third-party forensic specialists to identify what the script could do and determined on April 21, 2021 that the script was capable of capturing credit card information. We then worked to determine the window of time where credit card information could have potentially been exposed which concluded on July 21, 2021. The investigation confirmed there was a chance the unauthorized script present on our site may have exposed some of your personal information at point of sale. We are unable to confirm if any credit card transactions during this time period were affected.

What Information Was Involved? Our investigation has determined that orders processed via PayPal were not compromised and that the incident was limited to payments or attempted payments via credit card between February 3rd and March 16th. The potentially exposed data was limited to cardholder name, email address, billing address, credit card number, expiration date, and CVV.

What We Are Doing. As part of our security measures, we regularly screen activity on our website and continuously improve our security protocols. We will continue to enhance our security features to defend against security threats. In addition, we are also increasing the scrutiny of our third-party vendors and continuing to work with third-party forensics experts to prevent future incidents.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to 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 call our dedicated assistance line at 855-675-3097 between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday, excluding U.S. holidays. You may also email SCUF Gaming at data.controller@corsair.com.

Sincerely,

Team SCUF

Steps You Can Take to Protect Personal 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 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 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. SCUF Gaming is located at 3970 Johns Creek Court, Suite 325, Suwanee, GA 30024.

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; 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 XX Rhode Island residents impacted by this incident.