September 1, 2022 *Sent Via E-mail DOJ-CPB@doj.nh.gov

Mr. John M. Formella
New Hampshire Department of Justice (Office of Attorney General/ Consumer Protection)
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of Freestyle Solutions, Inc. Security Data Breach

Dear Mr. Formella:

We are writing to inform you that we recently became aware that cardholder information of customers of Joissu, Inc. was improperly accessed due to a security breach on the servers of Freestyle Solutions, Inc. We received a report from Freestyle Solutions Inc. on August 3, 2022 with a summary of the customers of Joissu, Inc whose information may have been subject to unauthorized access and use from September 2020 to February 2022 while the IIStealer malware resided on Freestyle Solutions, Inc. servers unnoticed.

The IIStealer malware captured information entered into the checkout page, including first and last name, payment card number, expiration date, security code, billing address, gift certificate number (if applicable), and transaction details. Joissu estimates that approximately 4,264 of its customers have been potentially affected by the data incident, 11 of whom are New Hampshire residents. A copy of the notice to customers required under N.H. Rev. Stat. § 359-C:20 is enclosed.

Joissu's notice to customers advises of immediate steps they can take to protect themselves from any potential harm resulting from the data incident. These steps include registering a fraud alert with the three major credit bureaus and encouragement to actively monitor accounts, and credit bureau reports. Joissu has also referred customers to the Federal Trade Commission's Identity Theft website, and the Office of the New Hampshire Attorney General Consumer Protection Bureau's website.

Joissu has and continues to take prompt action to investigate the incident, assess and mitigate risk to its customers, and improve its security, including transitioning to a new provider for the services previously provided by Freestyle Solutions, Inc. We greatly value the privacy and security of the information of our customers and are diligently working to ensure the aforementioned incident is properly addressed. If your office has any questions about this data incident, please contact Bret Clemons, President by e-mail at Bret.Clemons@joissu.com, phone to (407) 648-8746, or by mail to Joissu, Inc. 4637 LB Mcleod Rd, Orlando, Florida 32811.

Sincerely,

Bret Clemons
President, Joissu, Inc.

Enclosure: Notice to Customers

September 1, 2022

SENT VIA E-MAIL

Dear Customer:

We are writing to alert you of a data security breach experienced by one of our third party vendor's, Freestyle Solutions, Inc. ("Freestyle") involving the presence of malware on Freestyle's servers. Freestyle through SiteLINK provides the shopping cart and payment processing functionality for various companies' e-commerce sites, including ours.

On August 3, 2022 we received from Freestyle a transaction report which identified you as one of our customer's whose information was compromised as part of the security breach of Freestyle's servers. Freestyle has assured us that the malware was removed and additional steps were taken to block the unauthorized activity.

We are reaching out as our customers are a top priority, and we take the protection of your information very seriously. Below is additional information about what happened, what actions have been taken in response, and what steps you can take to further protect your information.

What Happened?

In early February 2022, Freestyle learned that IIStealer malware was identified on a server hosting one of its customer's website. Freestyle quickly commenced an investigation and identified and removed malware found on servers that hosted certain customers' e-commerce sites, including our website at https://www.joissu.com/.

Freestyle retained data security experts to conduct a thorough investigation of the incident's nature and scope and assist in Freestyle's containment and remediation efforts. Based on the investigation, Freestyle informed us the payment card information of 4,264 individuals who used a card on our site between September 2020 and February 3, 2022 may have been acquired by an unauthorized party.

What Information Was Involved?

The IIStealer malware captured information entered into the checkout page, including first and last name, payment card number, expiration date, security code, billing address, gift certificate number (if applicable), and transaction details (such as product type, price and quantity). According to Freestyle, there is no PIN input for debit card numbers on any SiteLINK checkout page and that information should not be at risk of having been compromised. Freestyle determined as part of its investigation that because the IIStealer malware captured the data as it was being submitted through the checkout form, this occurred immediately before it was encrypted for storage on Freestyle's database, the data was not encrypted at the time of capture.

Steps taken to Mitigate Harm

After becoming aware of the malware Freestyle took immediate steps to identify and remove

it and block further unauthorized activity. Freestyle launched an extensive investigation with the assistance of data security experts to determine the timeframes of exposure for each of Freestyle's affected customers and to identify impacted cardholders. Freestyle engaged Verizon to conduct a Payment Care Industry (PCI) Forensic Investigation. Freestyle also notified federal law enforcement authorities and has been coordinating with the payment card companies in an effort to protect affected cardholders. After receiving from Freestyle, on August 3, 2022, the transaction report identifying Joissu customers whose information may have been affected, we are actively reaching out to notify these customers. As an administrative, physical and technical precaution and security safeguard it has always been, and continues to be the policy and practice of Joissu, Inc. that we do not collect, maintain or store your personal cardholder information anywhere on our internal systems.

Although Freestyle took immediate action upon learning about the malware infiltration of its servers, we are disappointed they lacked the appropriate safeguards to prevent, or identify sooner such intrusion. For that reason we are working to end our vendor relationship with Freestyle, and will be transitioning to a new third party vendor for the services previously provided by Freestyle. Joissu has also undertaken itself to provide notice of the Freestyle's security breach to its affected customers where Freestyle did not do so, to provide required notices to the applicable department of the state for consumer protection, and to the major consumer reporting agencies that compile and maintain files on consumers on nationwide basis. Joissu has also asked for certification from Freestyle that its customers cardholder information is either destroyed and no longer stored on Freestyle servers, or that Freestyle provide justification why this information cannot be destroyed and confirm that the information will be appropriately safeguard to mitigate against future security breaches.

What You Can Do

Review Your Account Statements. We encourage you to remain vigilant by reviewing your account statements. If you believe there is an unauthorized charge on your card, please contact your financial institution or card issuer immediately. The payment card brands' policies provide that cardholders have zero liability for unauthorized charges that are reported in a timely manner. Please contact your card brand or issuing bank for more information about the policy that applies to you.

Review State and Federal Resource Websites. There are publicly available resources to assist you in protecting yourself from any potential harm, including identity theft. For example see:

- Federal Trade Commission https://www.identitytheft.gov/#/Info-Lost-or-Stolen
- Office of the New Hampshire Attorney General Consumer Protection Bureau https://www.doj.nh.gov/consumer/index.htm

Order a Credit Report. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228.

Consider Placing a Fraud Alert or Security Freeze on Your Credit File. To protect yourself

from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

You also have the right pursuant to 15 U.S.C. § 1681c-1 to place a "security freeze" on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.
The consumer reporting agencies may require proper identification prior to honoring your request.

For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For More Information

If you have any questions for about this issue, you can reach Joissu by e-mail at IncidentReport@joissu.com or call (407)-648-8746 Monday through Friday from 9 a.m. to 5 p.m.

To ask questions directly of Freestyle, the vendor who experienced the security breach please contact the SiteLINK response team at sitelinkquestions@freestylesolutions.com or 888-700-7498.

We hope this information is useful to you, and we sincerely regret any inconvenience or concern this may cause our customers.

Sincerely,

Bret Clemons

President, Joissu, Inc.