**Exhibit A**

**Consumer Notice Template**

<DATE>

<FIRST NAME> <LAST NAME>

<COMPANY>

<ADDRESS 1>

<ADDRESS 2>

<CITY>, <STATE> <ZIP CODE>

Dear <FIRST NAME>:

We are providing this notice to you pursuant to applicable law to notify you of a security incident regarding your Spreadshirt.com account.

# Approximate Date of Incident

We are still investigating and do not know the exact date of the security incident. We currently believe the security incident took place shortly before July 2021.

# Incident Overview

Early in July 2021 we discovered evidence of unauthorized access to employee computers. When we investigated this further, we concluded that a criminal deliberately targeted our network in an attempted ransomware attack.

We believe the attacker wanted to encrypt our systems and lock us out of them (which would make us unable to do business). This is a common type of malware attack against businesses. However, the attacker did not succeed.

Even so, we believe that the attacker was able to access and copy data from our internal networks. Therefore, there is a chance that the attacker will misuse or publish this data.

We do not know exactly what information the attacker was able to copy from our networks. Based on the evidence available right now, we believe the attacker was able to access internal business information as well as certain personal information. The types of personal information that might be affected are described below.

# Types of Personal Information Affected

To the extent that you had a partner account and actually entered the following data in your Partner Area, the attacker may have accessed your:

* First Name
* Last Name
* Address
* Phone Number
* Name of Bank Account Holder
* Bank Account Number
* Bank Name
* Bank Routing Number

We do not believe that your tax identification number (SSN if applicable) was accessed. This data is stored in a part of our network that we believe the attacker was not able to reach.

# Spreadshirt’s Remedial Measures

We immediately hired an external cybersecurity information technology company to analyze our systems, to help us stop the attack, and to help us to plan new security features for the future.

We have taken steps to secure access to our internal networks and to ensure no malware exists on our computers. Once we are sure that the attacker is not able to access our systems anymore, we will implement new security measures to reduce the impact from potential future attacks.

# How to Protect Your Personal Information

To protect yourself from any concrete harm as a result of this incident, you can:

* Monitor and notify your bank to be alert for any suspicious or potentially unauthorized activity in your accounts.
* Monitor your credit report. Be on the lookout for accounts you did not open, inquiries from creditors that you did not initiate, or inaccurate personal information. You can get a credit report for free at:

https://www.annualcreditreport.com/

* If you find suspicious activity on your credit reports or on your other account statements, consider placing a fraud alert on your credit files so creditors will contact you before opening new accounts. You can also implement freezes that will prevent new credit accounts from opening unless a PIN number is entered. You can place fraud alerts or apply freezes by contacting the three national credit reporting agencies.
* Ensure that you have strong, unique passwords for all of your accounts.
* Use Multi-Factor Authentication to log in to your accounts.

# Company Contact Information

You can call Spreadshirt, Inc. for more information at our toll-free customer service number:   
1-800-381-0815

You can also email Spreadshirt, Inc. at customersupport@spreadshirt.com.

We have a FAQ page about the incident here:   
https://help.spreadshirt.com/hc/en-us/articles/4403591449490

Sincerely,

Spreadshirt, Inc.  
1572 Roseytown Road  
Greensburg, PA 15601