



360 N. LA CIENEGA BLVD.
LOS ANGELES, CA 90048

HELLO@FABFITFUN.COM
855-313-6267

RECEIVED

JUN 02 2020

CONSUMER PROTECTION

May 27, 2020

By Certified Mail Return Receipt Requested

Attorney General
Consumer Protection & Antitrust Bureau
33 Capital Street
Concord, NH 03301

Re: Legal Notice of Personal Information Security Incident

Dear Sir or Madam,

FabFitFun, Inc. is sending you this letter to inform you of a recent incident during which certain consumer personal information was exposed.

Our technical team recently discovered that a third party had illegally placed malicious code on the <https://fabfitfun.com/shop/> extension of our website, using the administrative credentials of one of our employees. This code affected certain FabFitFun member information used on the Shop portion of the website. Our analysis has determined that the code was placed on the Shop portion of the site on May 2nd, and it was discovered shortly thereafter on May 6th as part of a routine review of our site. This portion of our website does not receive much traffic relative to the other portions of our website, so only a small number of customers, including four (4) New Hampshire customers, were impacted by this incident.

If a customer **completed a purchase** on the Shop site between May 2nd and May 6th of this year, we have reason to believe that their name, address, city, state, zip code, phone number, email address, credit card number, CVV code, and card expiration date were exposed.

If a customer was **in the process of checking out but did not complete a purchase** during this window, we have reason to believe that their name, address, city, state, zip code, phone number, and email address were exposed. We do not believe their credit card number, CVV code, and card expiration date were compromised, however, we are unable to confirm this.

We took immediate steps to mitigate this incident by removing the malicious code from our site and activating our incident response plan. We also conducted an internal investigation, and retained advisors to assist in the investigation and response. As with any incident of this nature, we are also of course reviewing our information security policies and practices to determine what, if anything, we can do to further guard against this type of intrusion and to improve site security. We are also conducting a comprehensive review of how the administrative credentials at issue were compromised and we will take appropriate remedial action depending on the outcome of that review. Lastly, we are preparing a mandatory privacy and security training module that will emphasize the importance of access controls and

log management.

We are in the process of notifying our affected customers and expect to make notification on May 25th. A copy of the notice being sent to the affected residents of your State is attached to this letter for your reference.

If you have any questions, please contact me at 310-935-0096 ext. 614 or shelly.gopaul@fabfitfun.com for more information.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Shelly Gopaul-Pettis', written in a cursive style.

Shelly Gopaul-Pettis
Assistant General Counsel
FabFitFun, Inc.

May __, 2020

<Affected Individual's Name>

<Address>

<City, State, Zip Code>

Dear <Affected Individual's Name>,

Notice of Data Breach

FabFitFun values your membership in our community and respects the privacy of your information, which is why we are writing to let you know about a recent data security incident that involves your personal information.

What Happened?

Our technical team recently discovered that a third party had illegally placed malicious code on the <https://fabfitfun.com/shop/> extension of our website. Our analysis has determined that the code was placed on the Shop portion of the site on May 2nd, and it was discovered shortly thereafter on May 6th as part of a routine review of our site. Shop was not highly trafficked at this time and the code did not impact other, more frequented portions of our website such as Add-Ons and Box purchases. Although only a very limited number of members were impacted, we have since been able to determine that you were likely one such member.

What Information was Involved?

If you **completed a purchase** on the Shop site between May 2nd and May 6th of this year, we have reason to believe that your name, address, city, state, zip code, phone number, email address, credit card number, CVV code, and card expiration date were exposed. Although we are not aware of any specific misuse of your information, we strongly urge you to take the steps detailed below.

If you were **in the process of checking out but did not complete a purchase** during this window, we have reason to believe that your name, address, city, state, zip code, phone number, and email address were exposed. We do not believe your credit card number, CVV code, and card expiration date were exposed, however, we are unable to confirm this with certainty. We are sending you this letter in an abundance of caution and we still urge you to take the steps detailed below.

What We are Doing

We took immediate steps to mitigate this incident by removing the malicious code from our site. We also activated our incident response plan, conducted an internal investigation, and retained advisors to assist in the investigation and response. As with any incident of this

nature, we are also of course reviewing our information security policies and practices to determine what, if anything, we can do to further guard against this type of intrusion and to improve site security.

We are deeply appreciative that you have chosen to be a part of the FabFitFun community and we are determined to make sure that you are happy with that decision. We are providing you with a complimentary one-year Annual Membership as a token of our appreciation for your business. At the end of your current membership, we will add four pre-paid boxes to your account and give you Select perks during that same time period. Once you have received the four pre-paid boxes, your original subscription will continue unless and until you decide otherwise.

What You Can Do

We urge you to immediately **contact your bank that issued your credit card** (the relevant phone number should be printed on the back of your card) and follow their recommendations. You should also closely **monitor your credit card account statements** for suspicious activity. If you see discrepancies or unusual activity, immediately call your bank. Under federal law and card company rules, customers who notify their payment card company in a timely manner upon discovering fraudulent charges will not be responsible for those charges.

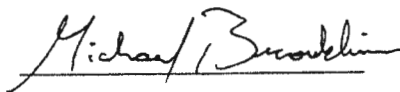
You may **report any fraudulent charges to your local police or sheriff's office** in order to file a police report for identity theft and to **obtain a copy of the report**. You may need to provide copies of the police report to creditors in order to clear any fraudulent charges from your records.

You can also take additional actions described on the attachment to this letter.

For More Information

If you have any questions, please contact our customer service team at 855-313-6267 or email privacy@fabfitfun.com for more information. We offer you our sincere apologies that this incident occurred.

Sincerely,

A handwritten signature in black ink that reads "Michael Broukhim". The signature is written in a cursive style with a horizontal line underneath the name.

Michael Broukhim, Co-CEO
FabFitFun, Inc.

Additional Important Information

For residents of Hawaii, Illinois, Iowa, Maryland, Michigan, Missouri, North Carolina, Virginia, and Vermont: It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident, and that you have rights pursuant to the federal Fair Credit Reporting Act. Please see the contact information for the Federal Trade Commission listed below.

For residents of Illinois, Maryland, North Carolina, and Rhode Island:

You can obtain information from the Maryland, North Carolina, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General

Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023

Rhode Island Office of the Attorney General

Consumer Protection
150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

North Carolina Office of the Attorney General

Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identitytheft.gov

For residents of Massachusetts and Rhode Island: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax ([https://assets.equifax.com/assets/personal/Fraud Alert Request Form.pdf](https://assets.equifax.com/assets/personal/Fraud%20Alert%20Request%20Form.pdf)), Experian (<https://www.experian.com/fraud/center.html>), or Transunion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/
800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013-9544
www.experian.com/freeze/center.html
888-397-3742

TransUnion (FVAD)

P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.