Cooley

Kris Kleiner
+1 720 566 4048
kkleiner@cooley.com

Via Email to: consumer@iowa.gov

September 18, 2020

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Legal Notice of Information Security Incident

Dear Sir or Madam:

I write on behalf of our client, FabFitFun, Inc. (the "Company"), to inform you of a potential security incident involving personal information for certain FabFitFun customers. FabFitFun has notified potentially affected individuals by email, including approximately seven hundred thirty Iowa residents, with mailed written notice to follow further outlining some steps they may take to help protect themselves.

FabFitFun recently discovered that an unauthorized third party inserted malicious code on portions of its website that may have enabled them to capture certain information in connection with customer sign ups. Based on forensic investigation, this incident affected new member sign up pages of the website during the period between April 26, 2020 and May 14, 2020, and between May 22, 2020 and August 3, 2020. This incident would have involved emails and FabFitFun passwords for customers that signed up using PayPal or Apple Pay. For customers using credit or debit cards, the information involved would also have included name, address, and payment card information. Although it appears that only a subset of members who signed up during this period would likely have been affected, FabFitFun is providing notifications to everyone that signed up during this timeframe as a precaution.

Upon learning of the incident, FabFitFun promptly took steps to address the situation, including removing the malicious code and taking steps to secure its website with the help of outside forensic cybersecurity experts engaged to assist FabFitFun in investigating and remediating the situation. In addition, FabFitFun is taking steps to help prevent this type of incident from happening again in the future. As an additional precaution, the Company has effected a password reset for all users. Finally, FabFitFun has reported the matter to law enforcement and will cooperate with the investigation.

As noted above, potentially affected individuals have been notified via email with written letter to follow, which we expect will begin mailing on or around September 22, 2020. A form copy of the letter being sent to the potentially affected Iowa residents is included for your reference. If you have any questions or need further information regarding this incident, please contact me at (720) 566-4058 or kkleiner@cooley.com.

Sincerely,

Kristopher Kleiner

Enclosure

<Name>
<Address>
<City, State, Zip Code>

<Date>

Dear <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 may involve your personal information. We previously sent an email regarding this incident and are providing this notice to potentially affected members to call their attention to steps they can take to help protect themselves. We take the security of personal information very seriously, and sincerely regret any concern this incident may cause.

What Happened?

Our technical team recently discovered that an unauthorized third party inserted malicious code on portions of our website that may have enabled them to capture certain information in connection with customer sign ups. Based on our forensic investigation, this incident concerns the new member sign up pages of our website during the period between April 26, 2020 and May 14, 2020, and between May 22, 2020 and August 3, 2020. According to our records, you signed up for FabFitFun during this timeframe, and your information therefore could have been affected. Although we believe that only a subset of members who signed up during this period were affected, we are notifying everyone that signed up during this timeframe as a precaution.

What Information was Involved?

This incident would have involved emails and FabFitFun passwords for customers that signed up using PayPal or Apple Pay. For customers using credit or debit cards, the information involved would also have included name, address, payment card account number, card expiration date, and card verification code. Please note that because we do not collect highly sensitive personal information like Social Security Numbers, this type of information was not affected by this incident.

What We are Doing

We took steps to address and contain this incident promptly after it was discovered. As soon as our technical team identified the issue, we removed the malicious code and took steps to secure our website with the help of forensic cybersecurity experts engaged to assist with our investigation. We have also reported the matter to law enforcement and are cooperating with the investigation. While we are continuing to review and enhance our security measures, we are confident that the issue has been resolved and will no longer affect transactions on our website.

Although Social Security numbers and other highly sensitive personal information were not at risk in this incident, as a precaution, we are making available to you one year of complimentary identity protection services from a leading identity monitoring services company. These services help detect possible misuse of your personal information and provide you with superior identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the enrollment instructions included with this letter.

We are deeply appreciative that you have chosen to be a part of the FabFitFun community, and as a token of that appreciation, we are also offering a $25 credit that can be used in an upcoming e-commerce sale. Information on

how you can redeem the credit was sent to you via email. Please note that you must be a current FabFitFun member to participate in our sales. You must also select, no later than December 31, 2020, the Winter sale to which you would like the credit to apply and the credit will expire if not used in the sale selected.

What You Can Do

- **Activating the Complimentary Identity Protection Services.** As outlined above, we are offering one year of identity theft protection and credit monitoring services at no charge to you. For more information about these services and instructions on completing the enrollment process, please refer to the "Information about Identity Theft Protection" reference guide attached to this letter. Note that you must complete the enrollment process by **December 31, 2020.**

- **Review Financial Account Statements.** You should review credit and debit card account statements as soon as possible in order to determine if there are any discrepancies or unusual activity listed. We urge you to remain vigilant and continue to monitor statements for unusual activity going forward. If you see anything you do not recognize, you should immediately notify the issuer of the credit or debit card as well as the proper law enforcement authorities. In instances of payment card fraud, it is important to note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.

- **Checking Credit Reports.** Although Social Security Numbers and other highly sensitive personal information were not at risk in this incident, as a general practice, we recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records.

- **Change Account Passwords.** As a further precaution, we have initiated a password reset for all FabFitFun users. You may have already been prompted to create a new password for your account. If you have not already done so, please do so now. As a reminder, you should use a unique and "strong" password for all online accounts. Tips on creating a strong password are available at http://www.connectsafely.org/tips-to-create-and-manage-strong-passwords/. In conjunction with the password reset, we are also implementing additional account protections, including additional password length and complexity requirements.

- **Consulting the Identity Theft Protection Guide. F**inally, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may wish to take to help protect yourself.

For More Information

If you have any questions, please contact our customer service team by using the chat function at the bottom of our website or by calling 855-313-6267. Once again, we sincerely regret that this incident occurred and any inconvenience or concern it may cause.

Sincerely,

Michael Broukhim
Co-founder and Co-CEO
FabFitFun

Information about Identity Theft Protection

To help protect your identity, we are offering a complimentary membership in Experian's® IdentityWorks®. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. Included with this service are fraud resolution services that provide an Experian Fraud Resolution agent to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). While this Fraud Resolution assistance is immediately available to you without any further action on your part, you can also activate the fraud detection tools available through enrolling in IdentityWorks® at no cost to you. To enroll in these services, visit: **www.experianidworks.com/credit** by **December 31, 2020**, and use the following activation code: **[ACTIVATION CODE]**. You may also enroll over the phone by calling **(877) 525-6943** between the hours of 9:00 AM and 9:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday (excluding holidays). Please provide the following engagement number as proof of eligibility: **DB22544.**

Once you enroll in IdentityWorks, you will have access to the following features:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance[1]:** Provides coverage for certain costs and unauthorized electronic fund transfers

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

Review Accounts and Credit Reports: You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of New York: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/internet/privacy-and-identity-theft.

---

[1] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

Security Freezes and Fraud Alerts: You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your 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 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports. By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may request that a freeze be placed on your credit report, at no charge, by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and an incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

Additional Information for New Mexico Residents: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. Here is a summary of your major rights under the FCRA:

- You have the right to be told if information in your file has been used against you;
- You have the right to receive a copy of your credit report and the right to ask for a credit score;
- You have the right to dispute incomplete or inaccurate information;
- You have the right to dispute inaccurate, incomplete, or unverifiable information;
- You have the right to have outdated negative information removed from your credit file;
- You have the right to limit access to your credit file;
- You have the right to limit "prescreened" offers of credit and insurance you get based on information in your credit report;
- You have the right to seek damages from violators; and
- You have the right to place a "security freeze" on your credit report.

For more information, including information about additional rights, you can visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf, https://www.consumerfinance.gov/learnmore/, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)
General Contact:
P.O. Box 740241, Atlanta, GA 30374
800-685-1111

Fraud Alerts and Security Freezes:
P.O. Box 740256, Atlanta, GA 30374

Experian (www.experian.com)
General Contact:
P.O. Box 2104, Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9556, Allen, TX 75013

TransUnion (www.transunion.com)
General Contact, Fraud Alerts and Security Freezes:
P.O. Box 2000, Chester, PA 19022
800-916-8800