



mwe.com

Scott Ferber
Attorney at Law
sferber@mwe.com
+1 202 756 8988

October 6, 2022

Attorney General Tom Miller
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319-0106
consumer@ag.iowa.gov

Re: **Data Security Incident**

Dear Attorney General Tom Miller,

As outside counsel for 32 Bar Blues LLC, we write to inform you of a data security incident that occurred on the systems of a PCI-certified third-party vendor, Freestyle Solutions, used by 32 Bar Blues for its website shopping cart solution. We also write to explain the steps that have been taken to address the incident.

On March 1, 2022, 32 Bar Blues received an email from Freestyle that Freestyle had identified malware on its own systems. Freestyle stated that it had promptly commenced an investigation and removed the malware from its systems on February 3, 2022 (within approximately 24 hours after becoming aware of it). According to Freestyle, the malware was first installed on its systems on September 18, 2020 and was designed to capture information entered on a website checkout page, including credit card information. Although Freestyle's March 1, 2022 email did not contain information regarding potentially affected individuals, as a precaution, 32 Bar Blues promptly notified its credit card payment processor / acquirer on March 3, 2022. On July 25, 2022, Freestyle provided, for the first time, transaction data, containing underlying details on potentially affected transactions, including information about the individual customers of 32 Bar Blues. Upon receiving this information, 32 Bar Blues engaged external support to assist with record deduping and address look ups. The review and address look up process was completed on about August 31, 2022. As a precautionary measure, 32 Bar Blues is now sending notice to the 77,303 individuals in the U.S., who were identified as having interacted with the

**McDermott
Will & Emery**

500 North Capitol Street, NW Washington DC 20001-1531 Tel +1 202 756 8000 Fax +1 202 756 8087

US practice conducted through McDermott Will & Emery LLP.

Freestyle solution between September 2020 and February 3, 2022. It is 32 Bar Blues' understanding that other companies using Freestyle also were impacted by the Freestyle incident.

Freestyle has advised that it has taken steps to contain the incident, fortify its controls, and further enhance its payment card security. Freestyle engaged Verizon to conduct a PCI Forensic Investigation and advise on containment and remediation activities. Freestyle also has notified the Cyber Fraud Task Force of the U.S. Secret Service's Chicago Field Office and has been coordinating with the payment card companies in an effort to protect affected cardholders.

Since being notified of the incident, 32 Bar Blues has worked to complete its review of the potentially affected data, engaging external support to assist with the review and locating up-to-date address information for identified individuals. The review and address look up process was completed on about August 31, 2022, with 32 Bar Blues' finding personal information for 578 state residents who interacted with the Freestyle solution between September 2020 and February 3, 2022. The personal information included name, address, payment card number, payment card expiration date, and payment card security code. To confirm, no social security numbers of 32 Bar Blues' customers were affected by the Freestyle data security incident.

32 Bar Blues is hereby notifying this Office and the individual state residents. The letters to residents are to be mailed by October 6, 2022. In addition, 32 Bar Blues has established a call center to answer notice recipient's questions.

Please do not hesitate to contact us if you have any questions regarding this letter.

Very truly yours,



Scott Ferber
202-756-8988

Attachment



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>>

NOTICE OF DATA BREACH

Re: **Important Security Notification**

Please read this letter.

Dear <<Name 1>>:

We are contacting you regarding a security incident that may have involved some of your personal information. We take the privacy and security of your personal information very seriously and for this reason want you to understand the steps we have taken to address this issue and additional steps you can take to protect yourself.

What Happened

32 Bar Blues recently learned that a Payment Card Industry (PCI)-certified vendor that it uses as its website shopping cart solution (Freestyle Solutions) was the victim of a data security incident. According to information provided by Freestyle, in early February 2022, Freestyle commenced an investigation and identified and removed malware that Freestyle found on its servers hosting e-commerce sites, which included 32BarBlues.com. Freestyle retained data security experts to assist in the investigation, including in evaluating the incident’s nature and scope and containing and remediating it. Based on the investigation that Freestyle conducted, it informed us that payment card information of individuals who used a card on 32BarBlues.com between September 2020 and February 3, 2022 may have been accessed without authorization.

What Information Was Involved

Based on its investigation, Freestyle has assessed that some of your personal information was in files that may have been accessed without authorization. This information may have included your name and the following: address, payment card number, payment card expiration date, and payment card security code.

What We Are Doing

As indicated above, after becoming aware of the issue, Freestyle took steps to identify and remove the malware and block further unauthorized activity. Freestyle launched an investigation with the assistance of its data security experts to determine the timeframes of potential exposure for each of Freestyle’s affected customers and to identify impacted cardholders. Freestyle also notified federal law enforcement authorities and has been coordinating with the payment card companies in an effort to protect affected cardholders. Upon being notified of the incident by Freestyle, 32 Bar Blues promptly notified its credit card payment processor / acquirer and engaged external support to assist with identifying its potentially affected customers.

What You Can Do

Please consider the following recommendations:

- **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.
- **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.

1901 Holser Walk, Unit 300, Oxnard, CA 93036
www.32BarBlues.com

- Review the Reference Guide. The attached Reference Guide provides additional recommendations on the protection of personal information.

More Information

Security, in all its forms, remains a top priority at 32 Bar Blues, and we will continue to take all appropriate steps to safeguard personal information and our systems. We apologize for any inconvenience or concern this incident may cause you. If you have any questions regarding this incident, please call 1-888-573-6902, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,
32 Bar Blues

Reference Guide

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus (Equifax, Experian and TransUnion) provide free annual credit reports only through the website, toll-free number or request form.

You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax
www.equifax.com
(800) 685-1111

Experian
www.experian.com
(888) 397-3742

TransUnion
www.transunion.com
(800) 916-8800

Upon receiving your credit report, review it carefully. Errors may be a warning sign of possible identity theft. Here are a few tips of what to look for:

- Look for accounts you did not open.
- Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case.
- Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidence of identity theft or fraud, promptly report the matter to your local law enforcement authorities (from whom you can obtain a police report), state Attorney General, and the Federal Trade Commission (FTC). You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
Bureau of Consumer Protection
600 Pennsylvania Avenue NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.ftc.gov/idtheft

Placing a Security Freeze

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.

You can place, temporarily lift, or permanently remove a security freeze on your credit report online, by phone, or by mail. You will need to provide certain personal information, such as address, date of birth, and Social Security number to request a security freeze and may be provided with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze. Information on how to place a security freeze with the credit reporting agencies is also contained in the links below:

<https://www.equifax.com/personal/credit-report-services/>

<https://www.experian.com/freeze/center.html>

<https://www.transunion.com/credit-freeze>

Fees associated with placing, temporarily lifting, or permanently removing a security freeze no longer apply at nationwide consumer reporting agencies.

Placing a Fraud Alert

To protect yourself from possible identity theft, 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 one-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. You may obtain additional information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or security freeze on your credit report.

IOWA RESIDENTS

You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at:

Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5164
www.iowaattorneygeneral.gov

MARYLAND RESIDENTS

You may obtain information about avoiding identity theft at:

Office of the State of Maryland Attorney General
Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.marylandattorneygeneral.gov

NEW MEXICO RESIDENTS

The Fair Credit Reporting Act provides certain rights in addition to the right to receive a copy of your credit report (including a free copy once every 12 months), including the right to ask for a credit score, dispute incomplete or inaccurate information, limit "prescreened" offers of credit and insurance, and seek damages from violators. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

NEW YORK RESIDENTS

You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
<https://ag.ny.gov/>

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
<https://ag.ny.gov/internet/resource-center>

NORTH CAROLINA RESIDENTS

You may obtain information about avoiding identity theft at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
919-716-6400
www.ncdoj.gov

OREGON RESIDENTS

We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
www.doj.state.or.us

RHODE ISLAND RESIDENTS

We first learned about a possible data security incident on July 26, 2022. Based on the investigation, personal information for 386 Rhode Island residents was in the potentially affected files. You may obtain information about avoiding identity theft at:

Office of the State of Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
401-274-4400
www.riag.ri.gov

You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.

WASHINGTON, D.C. RESIDENTS

You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
(202)-727-3400
www.oag.dc.gov