DAY PITNEY LLP

BOSTON CONNECTICUT FLORIDA NEW JERSEY NEW YORK PROVIDENCE WASHINGTON, DC

WILLIAM J. ROBERTS
Attorney at Law

242 Trumbull Street
Hartford, CT 06103-1212
T: (860) 275-0184 F: (860) 881-2431
wroberts@daypitney.com

Via Email

August 17, 2022

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

RE: Notification of Data Breach

Dear Iowa Office of the Attorney General Consumer Protection Division Director:

Pursuant to Iowa Code Ann. § 715C.2(8), on behalf of our client, Sturm, Ruger & Company, Inc. ("Ruger"), we are notifying the Iowa Office of the Attorney General of a data breach, affecting approximately 2,090 Iowa residents, that occurred at Freestyle Solutions ("Freestyle"), the third-party software vendor that owns and manages the server hosting ShopRuger.com, the online sportswear and accessories store for Ruger. You may also contact Freestyle directly regarding their data breach by calling 1 (800) 474-5760 or sending an email to SiteLINKQuestions@freestylesolutions.com or info@freestylesolutions.com. Our understanding is that Freestyle is represented by Brittany Bacon of Hunton Andrews Kurth LLP. Her contact information is bbacon@HuntonAK.com or 212-309-1361.

On August 2, 2022, Freestyle provided Ruger with a report detailing which ShopRuger customers' data was captured by malware that Freestyle had identified on the Freestyle server hosting the ShopRuger website. Based on its investigation of this data breach, Freestyle informed Ruger that the malware affected the Freestyle server used for the ShopRuger website from September 18, 2020 through February 3, 2022, the date upon which Freestyle removed the identified malware from its server.

Freestyle notified Ruger that the malware captured information entered by customers on the ShopRuger checkout page. The only items collected on the ShopRuger checkout page are: first and last name, shipping address, email address, payment card number, expiration

date, security code, billing address, gift certificate number (if applicable), description of the product purchased, price, and quantity. According to Freestyle, this data was captured when a customer clicked the "submission" button on the checkout form, immediately before the data was encrypted and stored in Freestyle's database.

Fortunately, the malware was limited to the Freestyle server and did not affect any system, computer, or server of Ruger itself. Information held by Ruger was completely unaffected by the Freestyle data breach.

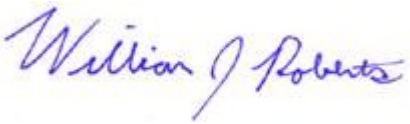
Freestyle notified Ruger that it has taken steps to contain the malware, including removing it from the server, blocking known malicious users, changing administrative passwords, and engaging Verizon to conduct an investigation and advise on further containment and remediation activities. Additionally, Freestyle informed Ruger that it has notified federal law enforcement authorities of this data breach and has been coordinating with payment card companies in an effort to protect affected cardholders.

Ruger has had several communications with Freestyle regarding its data breach to assist in our review of the matter, but we have been unable to obtain more detailed information. Ruger is in the process of notifying all affected customers and certain regulatory authorities in accordance with applicable law. Ruger will notify all affected customers by first class U.S. mail on August 18, 2022. A template copy of the notification being sent to affected customers is attached.

In addition, despite the fact that customers' Social Security numbers were not affected by this data breach (in fact, Ruger does not even collect such data), Ruger is offering all affected customers 12 months of identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 12 months of CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

I want to assure you that Ruger takes its obligation to protect the privacy and confidentiality of its customers' personal information very seriously and Ruger expects its vendors to do the same. If you have any questions, please contact me at 860-275-0184 or wroberts@daypitney.com.

Sincerely,



William J. Roberts
Attorney at Law
Day Pitney LLP

Return to IDX:
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1 (833) 423-2974
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

August 18, 2022

RE: Notice of Freestyle Solutions Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

Freestyle Solutions ("Freestyle") (www.freestylesolutions.com), the third-party software vendor that owns and manages the server hosting ShopRuger.com ("ShopRuger"), recently notified us that it experienced a data breach in which your payment card information was captured and potentially accessed by an unauthorized party. We are writing to provide information to you about Freestyle's data breach.

Although we have no evidence your information was used improperly, we are providing this notice out of an abundance of caution. Please see **Section 4**, below for more information. You may also contact Freestyle directly regarding their data breach by calling 1 (800) 474-5760 or sending an email to SiteLINKQuestions@freestylesolutions.com or info@freestylesolutions.com.

1. **Here is what happened:**

On August 2, 2022, Freestyle notified us that malware it identified on the Freestyle server hosting the ShopRuger website captured your information. Based on its investigation of this data breach, Freestyle informed us that the malware affected the Freestyle server used for the ShopRuger website from September 18, 2020 through February 3, 2022, the date upon which Freestyle removed the identified malware from its server.

Freestyle notified us that it has taken steps to contain the malware, including removing it from the server, blocking known malicious users, changing administrative passwords, and engaging Verizon to conduct an investigation and advise on further containment and remediation activities. Additionally, Freestyle informed us that it has notified federal law enforcement authorities of this data breach and has been coordinating with payment card companies in an effort to protect affected cardholders.

According to Freestyle, this malware was also identified on Freestyle servers hosting other of its customers' stores and is not unique to ShopRuger. This data breach did not involve any system or application managed by ShopRuger.

2. **How ShopRuger responded:**

On August 2, 2022, Freestyle provided us with a report detailing which ShopRuger customers' data was captured by the malware and potentially accessed by unauthorized parties. We have had several communications with Freestyle regarding its data breach to assist in our review of the matter, but have been unable to obtain more detailed information. ShopRuger has notified all affected customers and certain regulatory authorities in accordance with applicable law.

In addition, we are offering identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 12 months of CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

3. **Types of information involved:**

Freestyle notified us that the malware captured information entered by customers on the ShopRuger checkout page. The **only** items collected on the ShopRuger checkout page are: first and last name, shipping address, email address, payment card number, expiration date, security code, billing address, gift certificate number (if applicable), description of the product purchased, price, and quantity. **No other information whatsoever was involved in this data breach.** According to Freestyle, this data was captured when a customer clicked the "submission" button on the checkout form, immediately before the data was encrypted and stored in Freestyle's database.

4. **Protection of your information:**

We do not believe that your information is at risk or was improperly used because we have not received any notices from credit card companies or banks regarding fraudulent activity related to this data breach, or any customer complaints regarding this matter. Nevertheless, out of an abundance of caution, we have enclosed some general information about steps you can take to guard against identity theft and fraud.

We also encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1 (833) 423-2974 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is November 18, 2022.

5. **For more information:**

ShopRuger takes its obligation to protect the privacy and confidentiality of our customers' personal information very seriously and we expect our vendors to do the same. We sincerely regret that this data breach occurred. If you have any questions, you may contact IDX representatives who have been fully versed on the incident by calling 1 (833) 423-2974.

Sincerely,

Christopher J. Killoy
President & CEO
Sturm, Ruger & Company, Inc.

Reference Guide

We encourage customers affected by the Freestyle Solutions data breach to consider taking the following steps:

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. Most 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 Free 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, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. 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 consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies 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 consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert 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 2002 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

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit 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 fee for requesting, temporarily lifting, or permanently removing a security freeze with any of the consumer reporting agencies. 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.

Equifax	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	1-800-349-9960	www.equifax.com/personal/credit-report-services/
Experian	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/freeze/center.html
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-888-909-8872	www.transunion.com/credit-freeze

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)
- Social Security Card, pay stub, or W2
- 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.

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You may contact the Iowa Attorney General 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

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

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

For Massachusetts Residents. You have the right to obtain any police report filed in regard to this incident. 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 also place a security freeze on your credit reports, free of charge. 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 to place a security freeze on your account.

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

For 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

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to law enforcement and 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

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at:

Rhode Island Office of the Attorney General
Consumer Protection Unit
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.

For 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