RLF | RENZULLI LAW FIRM LLP

ONE NORTH BROADWAY, SUITE 1005
WHITE PLAINS, NY 10601
TEL (914) 285-0700 ■ FAX (914) 285-1213
www.renzullilaw.com

December 15, 2022

VIA E-MAIL (DOJ-CPB@doj.nh.gov)

Attorney General John Formella
Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capital Street
Concord, NH 03301

Re: Notice of Data Breach

Dear Attorney General Formella:

We are writing on behalf of our client, Steyr Arms, Inc. ("Steyr Arms"), to provide notification of a recent data breach.

Steyr Arms recently learned that certain customer and payment card information used to purchase products on its website may have been accessed by an unauthorized individual. In late August of 2022, a law enforcement agency notified Steyr Arms' parent company that an unauthorized Google Tag Manager ("GTM") code was identified on its website. Steyr Arms immediately identified and removed the code and commenced an investigation to determine, among other things, its purpose.

Steyr Arms retained data security experts to conduct a thorough investigation of the incident's nature and scope and to assist in Steyr Arms' containment and remediation efforts. Based on the investigation, customer and payment card information of individuals who made purchases on the website between June 15, 2022 and August 24, 2022 may have been acquired by an unauthorized party. The data security experts that Steyr Arms retained determined that because the malicious code captured the data as it was being submitted through the checkout form, which occurred immediately before the data was encrypted and submitted to Steyr Arms' payment processer, the data would not have been encrypted at the time of capture.

Steyr Arms received confirmation that consumer data was compromised from the data security experts it retained on November 17, 2022. The information potentially collected included first and last name, mailing addresses, billing addresses, and payment card data. On November 30, 2022, Steyr Arms confirmed the individuals who made purchases on the website during the relevant time period. Steyr Arms identified personal information related to ten New Hampshire residents who may have been impacted by this incident.

Beginning on December 21, 2022, Steyr Arms is providing written notice to all affected

consumers by mailing a letter via United States Postal Service First-Class mail. A sample copy of the consumer notification letter is enclosed.

Despite the fact that Social Security numbers were not affected by this data breach (and Steyr Arms does not even collect such data), Steyr Arms is offering all affected customers complimentary credit monitoring services for one year provided by Equifax. This service includes one year of unlimited access to Equifax credit reports and credit scores, daily credit monitoring services with notifications of any critical changes to a customer's credit file at Equifax, access to an identity restoration program that provides assistance in the event that a customer's identity is compromised, and up to $1,000,000 in identity theft insurance.

I want to assure you that Steyr Arms is committed to protecting the security and confidentiality of its customers' information and it has added an additional website security platform to enhance its ability to scan, monitor and react to any future data security threats.

If you have any questions, please contact me at (914) 285-0700 or pmalfa@renzullilaw.com.

Very truly yours,

RENZULLI LAW FIRM, LLP

Peter V. Malfa

Enclosure

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

Dear Customer:

We are writing to alert you of a data security breach regarding Steyr Arms, Inc.'s ("Steyr Arms") U.S. website, https://www.steyr-arms.com/us/, involving the presence of a malicious Google Tag Manager (GTM) code that was covertly implanted by an unknown party.

Our sales transaction records identify you as one of our customers whose information was comprised as part of the security breach of our website. Steyr Arms assures you that the GTM code was removed and additional steps were taken to block any additional unauthorized activity.

We are reaching out as our customers are a top priority, and we take the protection of your information very seriously. Below is additional information about what happened, what actions have been taken in response, and what steps you can take to further protect your information.

WHAT HAPPENED?

In late August of 2022, a law enforcement agency notified Steyr Arms' parent company that an unauthorized GTM code was identified on our website. We immediately identified and removed the code and commenced an investigation to determine, among other things, its purpose.

Steyr Arms retained data security experts to conduct a thorough investigation of the incident's nature and scope and to assist in Steyr Arms' containment and remediation efforts. Based on the investigation, customer and payment card information of individuals who made purchases on the website over a limited timeframe may have been acquired by an unauthorized party.

WHAT INFORMATION WAS INVOLVED?

The customer data that was compromised includes names, mailing addresses, billing addresses, and credit card numbers (including CCV codes and expiration dates) of customers who made purchases on our website between June 15, 2022 and August 24, 2022. The data security experts that Steyr Arms retained determined that because the malicious code captured the data as it was being submitted through the checkout form, which occurred immediately before the data was encrypted and submitted to Steyr Arms, the data would not have been encrypted at the time of capture.

WHAT WE ARE DOING.

After becoming aware of the GTM code, Steyr Arms took immediate steps to identify and remove it and block any further unauthorized activity. We launched an extensive investigation with the assistance of data security experts to determine whether and to what extent any customer information was exposed. After receiving the results of the data security experts' forensic investigation, Steyr Arms investigated its website transaction records to identify the names and addresses for customers whose information may have been affected. We are actively reaching out to notify the customers that have been identified. Steyr Arms has not and does not collect, maintain, or store payment card information anywhere on its website or internal systems.

Complimentary Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (1-Bureau Credit Watch Gold) for one year provided by Equifax.

To enroll in this service, go to the Equifax website at ***www.equifax.com/activate*** and in the space referenced as "Enter Activation Code", enter the following Activation Code **<<Insert Activation Code>>** and follow the steps to receive your credit monitoring service. Please see more information regarding the enrollment process at the end of this letter.

You can sign up for the credit monitoring service anytime between now and **March 31, 2023**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with Equifax, or an address in the United States and a valid Social Security number. Enrolling in this service will not affect your credit score. Once you are enrolled, you will be able to obtain one year of unlimited access to your Equifax credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at Equifax. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance. (Policy limitations and exclusions may apply.)

WHAT YOU CAN DO.

Fraud Alert Information

Whether or not you enroll in credit monitoring, we recommend that you place a "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two credit reporting companies so you do not need to contact each of them separately. The contact information for the nationwide credit reporting companies is:

Equifax	TransUnion	Experian
PO Box 740256	PO Box 2000	PO Box 9554
Atlanta, GA 30374	Chester, PA 19016	Allen, TX 75013
www.equifax.com	www.transunion.com/fraud	www.experian.com
1-800-525-6285	1-800-680-7289	1-888-397-3742

Free Credit Report Information
Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.
If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC at www.identitytheft.gov or at 1-877-ID-THEFT (1-877- 438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. Also visit the FTC's website at www.ftc.gov/idtheft to review their free identity theft resources such as their comprehensive step-by-step guide "*Identity Theft - A Recovery Plan*".

Security Freeze Information
You can request a "Security Freeze" on your credit file by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. When a Security Freeze is added to your credit report, all third parties, such as credit lenders, whose use is not exempt under law will not be able to access your credit report without your consent. The Security Freeze may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report. This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions and extension of credit at point of sale. There may be a fee for placing, temporarily lifting, or removing a Security Freeze, although that fee is waived if you send the credit reporting company proof of eligibility by mailing a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

To place a Security Freeze on your credit files at all three nationwide credit reporting companies, write to the addresses below and include the following information:

Equifax Security Freeze	TransUnion Security Freeze	Experian Security Freeze
PO Box 105788	PO Box 2000	PO Box 9554
Atlanta, GA 30348	Chester, PA 19016	Allen, TX 75013
www.freeze.equifax.com	www.transunion.com/freeze	www.experian.com/freeze
1-800-685-1111	1-888-909-8872	1-888-397-3742

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name (first, middle, last including applicable generation, such as Jr., Sr., III, etc)
- Your Social Security Number
- Your date of birth (month, day and year)
- Your complete address including proof of current address, such as a current utility bill, bank or insurance statement or telephone bill
- If you have moved, give your previous addresses where you have lived for the past 2 years

- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- Include applicable fee. Call or visit each of the credit reporting company websites listed above for information on fees for Security Freeze services. Forms of payment are check, money order, or credit card (American Express, Discover, MasterCard and Visa), or a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

Within 5 business days of receiving your request for a security freeze, the consumer credit reporting company will provide you with a personal identification number (PIN) or password to use if you choose to remove the freeze on your consumer credit report or to authorize the release of your credit report to a specific party or for a specified period after the freeze is in place.

FOR MORE INFORMATION.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New York Residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. State law advises you to report any suspected identity theft to law enforcement, as well as the FTC.

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

We regret that this incident has occurred. Your business is important to us. Please be assured that Steyr Arms is taking steps to ensure that a breach of this nature will not happen in the future. Please do not hesitate to contact our support agents for this event at 1-877-563-4718 if you have any further questions.

Sincerely

Dr. Michael Engesser
President & CEO
Steyr Arms, Inc.