

September 1, 2017

Consumer Protection & Antitrust Bureau  
33 Capitol Street  
Concord, NH 03301

To Whom It May Concern:

I represent WRJ Holdings, LLC, d/b/a Classic Firearms (“Classic”). This letter is being sent pursuant to N.H. Rev. Stat. Ann. §§ 359-C:19, -C:20, -C:21 because Classic learned, through forensic analysis that preliminarily determined on August 14, 2017 that a malicious attacker may have obtained payment card information of 66 New Hampshire residents from April 24 to June 8.

As soon as Classic suspected that its servers had been accessed without authorization, it engaged a digital forensics firm to shut down the affected server and investigate. It appears that a malicious attacker was able to modify a legitimate file to obtain access to Classic Firearms’ server, enabling the attacker to compile payment card information into a file for potential exfiltration. Classic could not confirm that this file was exfiltrated from its server or crossed company firewalls. While the forensic investigation was ongoing, Classic rebuilt, secured, and tested its server infrastructure to remove the threat and strengthen its security posture. Additionally, Classic is cooperating with law enforcement and notifying payment card networks.

Classic will begin notifying its customers on September 5, 2017 using the attached letter. As referenced in the letter, Classic will provide 12 months of identity repair and identity theft monitoring services to affected consumers through AllClear ID. Please contact me should you have any questions.

Sincerely,

Davis Wright Tremain LLP



Amy Mushahwar

cc: Rick Jones, Member



September 5, 2017

«First\_name» «Last\_name»  
«Address\_1», «Suite/Apt»  
«City», «State» «Zip»

### **NOTICE OF DATA BREACH**

Dear «First\_name» «Last\_name»,

We are writing to notify you about a security incident that may have resulted in the unauthorized acquisition of your payment card information.

**What Happened?** On June 8, 2017, we encountered a suspicious file on one of our servers. We immediately shut down the affected server and engaged forensic experts to begin an investigation to determine the cause and extent of the incident. Forensic analysis determined on August 14 that a malicious attacker could modify a legitimate file to obtain access to our server, enabling the attacker to compile payment card information into a file. This unauthorized access began on April 24 and lasted until June 8.

**What Information Was Involved?** The following personal information may have been accessed during the incident: first and last names, address(es), phone numbers, credit card numbers, credit card expiration dates, credit card identification numbers, and dates of birth.

**What We Are Doing.** Our forensic experts simultaneously began an investigation of the incident and assisted us in further securing our infrastructure. We are also cooperating with law enforcement.

We have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months:

**AllClear Identity Repair:** This service is automatically available to you with no enrollment required. If a problem arises, simply call 866-979-2595 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

**AllClear Identity Theft Monitoring:** This service offers additional layers of protection including identity theft monitoring that delivers secure, actionable alerts to you by phone and \$1 million identity theft insurance coverage. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at <http://enroll.allclearid.com> or by phone by calling 866-979-2595 using the following redemption code {Redemption\_Code}.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

**Other Important Information.** Please review the information on the reverse side of this letter which identifies additional steps to take to protect your information.

**For More Information.** For further information and assistance, please email us at [help@classicfirearms.com](mailto:help@classicfirearms.com) or contact Customer Support at 704-774-1104 from 9am to 5pm EST daily.

We care deeply about the privacy and security of your personal information. We regret any inconvenience this may cause you, and thank you for your understanding.

Sincerely,

Classic Firearms

(see reverse side)

**FURTHER STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION  
CONTACT LIST**

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities (from whom you may be able to obtain a police report), your state attorney general, and/or the Federal Trade Commission (FTC).

**Copy of Credit Report**

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>	<b>Free Annual Report</b>
P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	P.O. Box 1000 Chester, PA 19016 1-877-322-8228 www.transunion.com	P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 annualcreditreport.com

**Fraud Alert**

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

**Security Freeze**

In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you request a security freeze from a consumer reporting agency there may be a fee up to \$10 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

**Additional Free Resources on Identity Theft:** You can obtain information from the consumer reporting agencies, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

<b>Federal Trade Commission</b>	<b>Maryland Attorney General</b>	<b>North Carolina Attorney General</b>	<b>Rhode Island Attorney General</b>
600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and <a href="http://www.ftc.gov/idtheft">www.ftc.gov/idtheft</a> 1-877-438-4338	200 St. Paul Place Baltimore, MD 21202 <a href="http://www.oag.state.md.us">www.oag.state.md.us</a> 1-888-743-0023	9001 Mail Service Center Raleigh, NC 27699 <a href="http://www.ncdoj.gov">www.ncdoj.gov</a> 1-877-566-7226	150 South Main Street Providence, RI 02903 <a href="http://www.riag.ri.gov">www.riag.ri.gov</a> 401-274-4400

We will **NOT** send you any electronic communications regarding this incident and ask you to disclose any personal information.

Massachusetts residents have the right to obtain a police report.