Crimson Trace

ENHANCING PEOPLE'S ABILITY TO PROTECT FAMILY, HOME AND COUNTRY.

SAM A SAMPLE
123 ANY ST
SUITE 456
ANYCITY, USA 12345-6789

May 30, 2017

Dear Sam Sample,

Crimson Trace recently became aware of a data security incident that may have affected certain customers who made a purchase on www.crimsontrace.com. We are providing this notice to inform you about the incident and to call your attention to precautionary steps you can take. We take your privacy very seriously and sincerely regret any concern this matter may cause you.

**What Happened?**

An extensive forensic investigation found that an unauthorized individual was able to gain access to our website and may have compromised payment card information as well as some basic contact information of customers who transacted on the site between June 1, 2016 and May 5, 2017.

**What Information Was Involved?**

The customer information potentially affected by this incident includes name, billing address, email address, telephone number, payment card account number, payment card type, expiration date, and CVV code. We understand you may be concerned about this incident, but we would like to emphasize that we have no evidence that information about the specific products you purchased has been exposed.

**What We Are Doing**

We take the privacy and security of our customers' personal information very seriously and deeply regret that this incident occurred. We took immediate steps to address and contain this incident once it was discovered, including engaging outside forensic experts to assist us in investigating and containing the situation. We have also enhanced the security of our systems to prevent further incidents. While we continue to evaluate our security measures, we believe the incident has now been contained.

**What You Can Do**

- **Review Card Statements:** You should review credit and debit card account statements as soon as possible and remain vigilant in order to identify any discrepancies or unusual activity. If you see any transactions that you do not recognize, immediately notify the issuer of the credit or debit card. *In instances of payment card fraud, please note that cardholders are typically not responsible for any fraudulent activity that is reported in a timely fashion.*
- **Enrollment in Complimentary Identity Protection Services:** To help address concerns you may have following this incident, we have secured the services of global risk mitigation and response leaders, Kroll, to provide identity monitoring at no cost to you for one year. To enroll, please follow these steps:
  - Visit **kroll.idmonitoringservice.com** to activate and take advantage of your identity monitoring services.
  - You have until **August 31, 2017** to activate your identity monitoring services.
  - Please provide the following membership Number: **C123456789**
  - To receive credit services by mail instead of online, please call [redacted]. Additional information describing the Kroll services is included in the attachment to this letter.

- **Information About Identity Theft Protection Guide:** Please review the "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself.

**For More Information**

If you have additional questions or concerns about this incident you may contact us at [redacted] between 9:00 a.m. and 6:00 p.m. Eastern time, Monday through Friday. Again, we sincerely regret any concern this event may cause you.

Sincerely,

Nate Hoke
Director, Customer Service

## Information About Identity Theft Protection

**Credit Monitoring:** You've been provided with access to the following services from Kroll:

- **Single Bureau Credit Monitoring –** You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.
- **Web Watcher –** Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.
- **Public Persona –** Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.
- **Quick Cash Scan –** Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.
- **$1 Million Identity Fraud Loss Reimbursement –** Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.
- **Fraud Consultation –** You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.
- **Identity Theft Restoration –** If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

**Review Accounts and Credit Reports:** As a precaution, you may 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 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.

**Fraud Alerts:** There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven 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.

**Credit Freezes:** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

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)**
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

**Fraud Alerts:**
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
**Credit Freezes:**
https://www.freeze.equifax.com

**Experian (www.experian.com)**
P.O. Box 2002
Allen, TX 75013
888-397-3742

**Fraud Alerts:**
https://www.experian.com/fraud/center.html
**Credit Freezes:**
https://www.experian.com/consumer/security_freeze.html

**TransUnion (www.transunion.com)**
P.O. Box 1000
Chester, PA 19016
800-888-4213

**Fraud Alerts:**
http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page
**Credit Freezes:**
http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.