MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

M. Alexandra Belton
Office: (267) 930-4773
Fax: (267) 930-4771
Email: abelton@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

June 26, 2019

INTENDED FOR ADDRESSEE(S) ONLY

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

Our firm represents A.T. Cross Company ("A.T. Cross"), 299 Promenade Street, Providence, RI 02908, and we write to notify your Office of an incident that may affect the security of payment card information relating to five (5) New Hampshire residents. The investigation into this matter is ongoing and this notice will be supplemented with any substantive facts learned subsequent to its submission. By providing this notice, A.T. Cross does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

In May 2019, A.T. Cross received reports from certain customers that the checkout page of its website was behaving abnormally. A.T. Cross immediately took steps to investigate this issue. A.T. Cross also began working with its website support vendors and third-party forensic experts to confirm the nature and scope of the incident. Based on the results of the forensic investigation, on or around June 3, 2019, A.T. Cross confirmed that payment card data, including customer name, address, card number, expiration data and security code, used for purchases on *www.cross.com* between May 9 and May 14, 2019 was potentially subject to unauthorized acquisition. Following a review of the online purchases made during that window, A.T. Cross identified payment card information belonging to five (5) New Hampshire residents was used for purchases on the site during the relevant time frame.

Notice to New Hampshire Residents

On or about June 26, 2019, A.T. Cross provided written notice of this incident to all affected individuals, which includes five (5) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

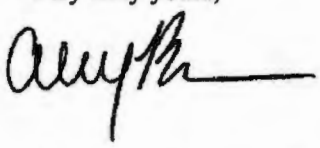
Upon learning of an issue with its website check out page, A.T. Cross immediately took steps to ensure the security of its site and investigate the issue. This effort included working with its website support vendors, as well as third-party forensic investigators. A.T. Cross also worked quickly to identify and notify those customers whose information may have been used on the site during the relevant timeframe. While it has safeguards in place, A.T. Cross is reviewing its security measures to ensure the ongoing security of its systems.

A.T. Cross is also providing impacted individuals with guidance on how to better protect against misuse of payment card information, as well as identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. A.T. Cross is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. A.T. Cross notified its payment card transaction processor about the incident immediately upon discovery. A.T. Cross is also notifying other regulatory agencies, as appropriate.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4773.

Very truly yours,



M. Alexandra Belton of
MULLEN COUGHLIN LLC

MAB/nsj
Enclosure

EXHIBIT A

A.T. CROSS COMPANY

CROSS. SHEAFFER.

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>>

RE: NOTICE OF DATA BREACH

Dear <<Name 1>>:

A.T. Cross Company ("A.T. Cross") writes to notify you of a recent incident that may affect the security of your payment card information. We take this incident very seriously and are providing you with details about the incident, our response, and steps you can take to better protect your personal information, should you feel it appropriate to do so.

What Happened? In May 2019, A.T. Cross received reports from certain customers that the checkout page of its website was behaving abnormally. A.T. Cross immediately took steps to investigate this issue. We also began working with our website support vendors and third-party forensic experts to confirm the nature and scope of the incident. Based on the results of the forensic investigation, on or around June 3, 2019, we confirmed that card data, including customer name, address, card number, expiration data and security code, used for purchases on *www.cross.com* between May 9 and May 14, 2019 were potentially subject to unauthorized acquisition. We then undertook an internal review to identify those customers who made purchases during that time.

What Information Was Involved? Our investigation determined that your name, address, credit/debit card number, expiration date and security code were potentially acquired without authorization.

What We Are Doing. A.T. Cross takes the security of information in our care very seriously. Upon learning of the incident, we immediately took steps to ensure the security of our website and investigate the issue. We are reviewing the security measures in place to ensure the ongoing security of our systems. We are also providing you with information about this event and about the steps you can take to better protect against misuse of your payment card information, should you feel it appropriate to do so.

What You Can Do. We encourage you to review the enclosed "Privacy Safeguards" which includes guidance on steps you can take to better protect against misuse of your information.

For More Information. We understand you may have questions or concerns that are not addressed in this letter. If you have additional questions, you may call our dedicated call center we have established regarding this incident at 877-641-8844. The call center is available Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time, excluding U.S. holidays.

Again, we take this incident seriously and sincerely regret any inconvenience or concern this incident has caused you.

Regards,

Karl Pearson

Karl Pearson, CEO
A.T. Cross Company

PRIVACY SAFEGUARDS

Monitor Accounts. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Security Freeze. You have the 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. 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.

Fraud Alert. As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-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. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information. You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us. A.T. Cross Company can be reached by mail at 299 Promenade Street, Providence, RI 02908.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 10 Rhode Island residents impacted by this incident.