



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

MAR 16 2020

CONSUMER PROTECTION

Christopher J. DiIenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

March 10, 2020

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

Re: **Notice of Data Event**

Dear Sir or Madam:

We represent TrueFire LLC ("TrueFire") located at 2500 Emerson Ave. S., St. Petersburg, FL 33712, and are writing to notify your office of an incident that may affect the security of some personal information relating to twenty-eight (28) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, TrueFire 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

On January 10, 2020, TrueFire discovered that an unauthorized person gained access to certain information that consumers had entered through its website. While TrueFire does not store credit card information on its website, it appears that the unauthorized person gained access to the website and could have accessed the data of consumers who made payment card purchases, while that data was being entered. This occurred between August 3, 2019 and January 14, 2020. The information that could have been subject to unauthorized access includes name, address, payment card account number, card expiration data and security code.

Notice to New Hampshire Residents

On or about March 10, 2020, TrueFire provided written notice of this incident to the affected twenty-eight (28) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Mullen.law

Other Steps Taken and To Be Taken

Upon discovering the event, TrueFire moved quickly to investigate and respond to the incident, assess the security of TrueFire systems, and notify potentially affected individuals. TrueFire is also working to implement additional safeguards and data privacy training to its employees.

TrueFire is providing impacted individuals with guidance on how to better protect against 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. TrueFire is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. TrueFire is also providing notice of this incident to any regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4775.

Very truly yours,

A handwritten signature in black ink, appearing to read 'C. DiLenno', with a stylized flourish at the end.

Christopher J. DiLenno of
MULLEN COUGHLIN LLC

CJD:ncl
Enclosure

EXHIBIT A



Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741



[FIRST NAME] [LAST NAME]
[ADDRESS_1]
[ADDRESS_2]
[CITY], [ST] [ZIP CODE]

March 9, 2020

Re: Notice of Data Breach

Dear [FIRST NAME] [LAST NAME]

TrueFire LLC (“TrueFire”) is writing to inform you of an incident that may affect certain personal information you provided while making a purchase at TrueFire.com (the “Website”). As a precaution, we are providing this notice and outlining some steps you may take to help protect yourself. We truly apologize for any inconvenience or concern this may cause you.

What happened? On January 10, 2020, TrueFire discovered that an unauthorized person gained access to our computer system and, more specifically, to information that consumers had entered through the Website. While we do not store credit card information on our website, it appears that the unauthorized person gained access to the Website and could have accessed the data of consumers who made payment card purchases, while that data was being entered, between August 3, 2019 and January 14, 2020.

What Information Was Involved? We cannot state with certainty that your data was specifically accessed, however you should know that the information that was potentially subject to unauthorized access includes your: name, address, payment card account number, card expiration data and security code.

What are we doing? We take the privacy and protection of personal information very seriously. As soon as we discovered the incident, we immediately took steps to address it, including working with computer forensic specialists to determine the full nature and scope of the intrusion and reporting the incident to law enforcement. We are continuing to monitor all activity on the Website to ensure the intrusion remains contained, and are working with an outside computer forensic team to monitor, remediate and identify any issues.

What can you do? We want to make you aware of steps you can take to guard against identity theft and fraud. Please review the enclosed Information about Identity Theft Protection. We also recommend that you review your credit and debit card accounts statements to determine if there are any discrepancies or unusual activity listed. You should also remain vigilant and continue to monitor your statements for unusual activity going forward. If you see anything you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately to report the issue.

For More Information. We understand that you may have questions about the incident that are not be addressed in this letter. If you have additional questions, or need assistance, you may contact us at 877-423-5870 from 9:00 am ET to 7:00 pm ET Monday through Friday. Again, we apologize for any inconvenience or concern this event may have caused.

Sincerely,

A handwritten signature in black ink, appearing to read "Ren Wright", with a large, sweeping flourish extending to the right.

Ren Wright
Chief Customer Officer
TrueFire LLC

TFS-MULTI

Information about Identity Theft Protection

We encourage you to remain vigilant against incidents of identity theft, to review your account statements, and to monitor your credit reports and explanation of benefits forms 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.

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:

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-909-8872
www.transunion.com/credit-freeze

Experian

PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

Equifax

PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
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;

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit file report, based upon the method of the request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with the process by which you may remove the security freeze, including an authentication mechanism. Upon receiving a direct request from you to remove a security freeze and upon receiving proper identification from you, the consumer reporting agency shall remove a security freeze within one (1) hour after receiving the request by telephone for removal or within three (3) business days after receiving the request by mail for removal.

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:

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

You can also 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, your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438-4338); and TTY: 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 also obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

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 New Mexico: 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 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 residents of New York: 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/>.

For residents of Rhode Island: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are twenty-one Rhode Island residents impacted by this incident.