



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

NOV 19 2018

CONSUMER PROTECTION

James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

November 14, 2018

INTENDED FOR ADDRESSEE(S) ONLY

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Hats.com located at 110 East Main Street, PO Box 517, Adamstown, PA 19501, and are writing to notify your office of an incident that may affect the security of some personal information relating to 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, Hats.com 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 or about September 23, 2018, Hats.com became aware that certain personal data entered on either of their websites, Hats.com and Kangol.com, was being acquired by an unauthorized user as a result of malware placed on the affected websites. We immediately launched an investigation to determine what happened and what information was affected. With the assistance of computer forensics experts, we learned that both websites were the victim of a malware event. The event resulted in the unauthorized acquisition of our customers name, address and credit card information which was entered on either website between August 18, 2018 and September 23, 2018. On October 18, 2018 our third party forensic investigation confirmed that this information was subject to unauthorized access or acquisition and that said information related to New Hampshire residents. Although we are unaware of any actual or attempted misuse of this personal

Attorney General Gordon J. MacDonald
November 14, 2018
Page 2

information, we notified affected individuals because their information was subject to unauthorized access or acquisition through either of the websites during the affected period.

The information that could have been subject to unauthorized access includes name, address, and credit card information.

Notice to New Hampshire Residents

On or about November 14, 2018, Hats.com began providing written notice of this incident to affected individuals, which includes seven (7) 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 discovering the event, Hats.com moved quickly to investigate and respond to the incident, assess the security of Hats.com systems, and notify potentially affected individuals. Hats.com reset passwords for all administrative accounts, implemented increased security measures for website administrative access, updated our infrastructure, conducted additional employee training, and are currently reviewing our policies and procedures relating to data security.

Additionally, Hats.com 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. Hats.com is also 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4798.

Very truly yours,



James E. Prendergast of
MULLEN COUGHLIN LLC

JEP:mal
Enclosure

EXHIBIT A

[Hats.com, LLC Letterhead]

[date]

[name]

[address]

RE: Notice of Data Breach

Dear [name]:

Hats.com, LLC (“Hats.com”) which operates the website [Company/affected website] is writing to notify you of an incident that may affect the security of your personal information. We are providing you with information regarding the incident, steps we have taken since discovering the incident, and what you can do to protect your personal information should you feel it is appropriate to do so.

What Happened? On or about September 23, 2018, Hats.com became aware that certain personal data entered on the [Company/affected website] website was being acquired by an unauthorized user as a result of malware placed on the affected website. We immediately launched an investigation to determine what happened and what information was affected. With the assistance of computer forensics experts, we learned Hats.com was the victim of a malware event on its website, [Company/affected website]. The event resulted in unauthorized acquisition of your name, address and credit card information which you entered on this website between August 18, 2018 and September 23, 2018. On October 18, 2018 our forensic investigation confirmed that this information was subject to unauthorized access or acquisition. Although we are unaware of any actual or attempted misuse of this personal information, we are notifying you in an abundance of caution because your information was entered on the website during the affected period.

What Information Was Involved? Hats.com is not aware of any actual or attempted misuse of your information; however, our investigation confirmed the information subject to unauthorized acquisition includes your name, address, and credit card information.

What We Are Doing. Information privacy and security are among our highest priorities. Hats.com has strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to confirm the security of our systems, including our website. We reset passwords for all administrative accounts, implemented increased security measures for website administrative access, updated our infrastructure, conducted additional employee training, and are currently reviewing our policies and procedures relating to data security. In an abundance of caution, we are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so.

What You Can Do. You may review the information contained in the attached “Steps You Can Take to Protect Your Information.” You can also stay aware and monitor any unusual activity on your credit report.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If so, you may contact our call center at (877) 216-4023 which is available Monday through Friday from 9:00am – 7:00pm (Eastern time).

We regret sincerely the inconvenience this incident causes for you. Hats.com remains committed to safeguarding information in our care and will continue to take proactive steps to enhance data security.

Sincerely,

Donald Rongione
President and CEO
Hats.com, LLC

Enclosure

Steps You Can Take to Protect Against Identity Theft and Fraud

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.

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 PO Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-909-8872 www.transunion.com/credit-freeze	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.

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 P.O. Box 2002 Allen, TX 75013 1-888-397-3742	TransUnion P.O. Box 2000 Chester, PA 19106 1-800-680-7289	Equifax P.O. Box 105069 Atlanta, GA 30348 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

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more 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.

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 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 XXX Rhode Island residents impacted by this incident.