Subject: Data Breach Notification

EnChroma Inc. is a California corporation that sells eyewear to customers in the US and worldwide via its website, enchroma.com. On or about May 15th 2018 a hacker was able to insert program code into a file on our website system. The program code caused customer personal information and payment information to be saved into a file stored on the web server. On or about May 17th 2018 the hacker downloaded the file using an IP address apparently located in the Denmark according to WHOIS lookup.

We first became aware of the situation on May 17th when IT staff detected that an unauthorized alteration had been made to a program file on the web server. All program files are stored in a version control system (VCS). The VCS alerted us to the fact that said file had been modified. According to our best available information the modification was in place for approximately 72 hours.

The access log of the hacker is attached to this email for your review.

How many New Hampshire residents affected?

There were only 2 New Hampshire residents affected.

What is the anticipated date of notice?

Enchroma's primary means of communications with the affected New Hampshire residents is by electronic means. A sample copy of the email notifications sent to the affected New Hampshire residents on June 27, 2018, is attached to this message. Written notices containing substantially the same content as the email notifications were also sent via USPS on the same date.

Sincerely,

Andrew Schmeder
CEO, EnChroma, Inc.

enchroma.

[redacted]>

Re: Notice of Data Breach

1 message

EnChroma Customer Support <support@enchroma.com> [redacted]
Reply-To: EnChroma Customer Support <support@enchroma.com>
[redacted]

Dear [redacted],

We are writing to notify you that a data breach occurred on our website which caused the unauthorized acquisition of your personal and payment information on or around May 15, 2018, to May 17, 2018.

What Happened?

On or about May 15th, 2018, a hacker infiltrated our website systems and inserted a malware. The malware caused certain customers' personal information and payment information to be saved into a file stored on our web server. Unfortunately, your personal information was compromised as a result of this infiltration. On or about May 17th 2018 the hacker downloaded the file. We became aware of the attack on May 17th, 2018 and immediately disabled it. According to our best available information, the malware was in place for approximately 72 hours before we were able to disable it.

What Information Was Involved?

The personal information and payment information downloaded by the hacker may include your full name, shipping address, billing address, telephone number, credit card number, expiration date, CVC code, and email address. To the best of our knowledge, no login names or passwords, or information about past orders or test results were stolen.

What We Are Doing.

We take the privacy and security of our customer's information very seriously. Immediately upon learning of the incident, we completely shut down and quarantined the computer system that was infiltrated. We have also migrated our entire website to a completely new, secure third-party platform so that there is no possibility of code contamination.

What You Can Do.

Firstly, we encourage you to contact your credit card company to obtain a new card number. We also encourage you to remain vigilant over the next twelve to twenty-four months. Review your account statements, promptly report incidents of suspected theft to the credit card company, and monitor your credit reports for suspicious activity.

1. Credit Reports

You are entitled to one free credit report annually from each of the three major credit reporting agencies. To order your free credit report, visit www.annualcreditreport.com.

At no charge, you may also place a "fraud alert" on your credit file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Please note that placing a fraud alert may delay your ability to obtain credit while the credit agency verifies your identity. As soon as one credit agency confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact one of the agencies listed below.

Equifax
800-685-1111
www.equifax.com

Experian
888-397-3742
www.experian.com

TransUnion

800-680-7289
www.transunion.com

2. Security Freeze

Under your state law, you as a consumer may place a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

Depending on the state in which you reside, a credit reporting agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You can determine the fees for your particular state at: https://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000

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 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;

8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to

you when you placed the security freeze. The credit agencies have three business days after receiving your request to remove the security freeze.

For More Information.

You can educate yourself regarding identity theft and the steps you can take to protect yourself by contacting your state Attorney General or the Federal Trade Commission ("FTC"). The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/miscorsites/idtheft/, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your state Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state Attorney General.

We sincerely apologize for any inconvenience this may cause you and regret that this situation occurred. Your confidence in our ability to safeguard your personal information and your peace of mind are very important to us. Should you have any questions or concerns regarding this matter or the protections available to you, please call us at **510-497-0048** during our normal business hours.

Respectfully,

Andrew Schmeder
President & CEO,
EnChroma, Inc.