

NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
799 9th Street NW
Suite 1000
Washington, DC 20001-4501
United States
Direct line +1 202 662 4691
chris.cwalina@nortonrosefulbright.com
Tel +1 202 662 0200
Fax +1 202 662 4643
nortonrosefulbright.com

July 19, 2018

Via FedEx

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

RECEIVED

JUL 20 2018

CONSUMER PROTECTION

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

Pursuant to N.H. Rev. Stat. § 359-C:20, I write on behalf of my client, Helly Hansen A.S (a Norwegian registered company) ("Helly Hansen"), to notify you of a security incident which may have resulted in unauthorized acquisition of payment card data of ten (10) New Hampshire residents. Helly Hansen takes the protection of its customers personal information very seriously and is taking steps to notify potentially affected individuals, and provide them with information to help protect their information.

Based on Helly Hansen's investigation to date, Helly Hansen has learned that from April 20, 2018 to April 26, 2018 and from May 2, 2018 to May 14, 2018, its e-commerce website, hellyhansen.com, was exposed to malware. During these periods, Helly Hansen believes the malware had the potential to obtain information entered online to make a purchase including first and last name, street, city, region, country, postal code, telephone number, credit card number, expiration date, and card verification code. As soon as the malware was discovered (following a release of a patch by the website platform provider, Magento), it was contained and remediated. Helly Hansen immediately launched a thorough investigation and engaged the assistance of a forensic firm to determine the capabilities of the malware and determine what information was potentially exposed.

While the investigation is still ongoing, Helly Hansen believes that the malware had the potential to capture the data elements listed above for purchases made on hellyhansen.com during the limited timeframes outlined above. If these date ranges change, we will notify those affected.

At this time Helly Hansen has no evidence that any payment card information has been misused. However, in an abundance of caution, Helly Hansen has notified New Hampshire residents who purchased items on hellyhansen.com during the noted date range.

Helly Hansen is also conducting a thorough review of its security measures, internal controls, and safeguards and is making changes to help prevent a similar incident in the future.

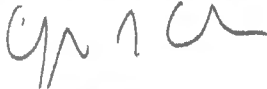
Affected individuals are being notified via email. A form copy of the email provided to affected New Hampshire residents is included for your reference.

Below is the contact information for James Brook, Group General Counsel, at Helly Hansen:

James Brook
Group General Counsel
James.brook@hellyhansen.com
International House
St Katharine Docks,
London E1W 1UN
+44 7525 080 801

If you have any questions or need further information regarding this incident, please contact me at (202) 662 4691 or chris.cwalina@nortonrosefulbright.com.

Very truly yours,



Chris Cwalina

CGC/
Enclosure

RE: Notice of Data Security Incident

Dear [Insert Recipient's Name]:

We are writing to let you know about a data security incident, which may have resulted in unauthorized access to certain contact and payment card information, and to provide you with steps you can take to protect yourself from possible misuse of your information.

What Happened

Based on our investigation to date, we learned that from April 20, 2018 to April 26, 2018 and from May 2, 2018 to May 14, 2018, our e-commerce website, hellyhansen.com, was exposed to malware that we believe had the potential to obtain information entered online to make a purchase.

What Information Was Involved

While our investigation is ongoing, we believe that the malware at issue could have captured your first and last name, street, city, region, country, postal code, telephone number, credit card number, expiration date, and customer verification code.

What are We Doing

As soon as we learned of the malware, we quickly took measures to contain and eradicate the malware that was present, and are working to further enhance our security measures. We have also notified the appropriate regulatory authorities.

What You Can Do

We recommend that you review your bank account and credit card statements and notify your bank or credit card company if you identify any suspicious activity. Be sure to immediately report any unauthorized charges to your card issuer. The phone number to call is usually on the back of your payment card.

Please see the section that follows this notice for additional steps you may take to protect your information. The additional information section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information

If you have any questions, please contact your dedicated Helly Hansen team at dataprivacy@hellyhansen.com.

While we sincerely regret that this incident has occurred, we are taking every step to ensure that your interest is served first and are working hard to earn the trust you place in us.

Yours sincerely,

Paul Stoneham,
CEO
Helly Hansen AS

Additional Information

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax

Phone: 1-800-685-1111
P.O. Box 740256
Atlanta, Georgia 30348
www.equifax.com

Experian

Phone: 888-397-3742
P.O. Box 9554
Allen, Texas 75013
www.experian.com

TransUnion

Phone: 888-909-8872
P.O. Box 105281
Atlanta, GA 30348-5281
www.transunion.com

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW
Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If you are a resident of Iowa, you may contact the Iowa Attorney General's Office at the Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, Email: consumer@ag.iowa.gov; Telephone: 515-281-5926 or 888-777-4590 (outside of the Des Moines metro area).

If you are a resident of Maryland, you may contact the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202; Website: www.oag.state.md.us; Telephone: 1-888-743-0023.

If you are a resident of North Carolina, you may contact the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699; Website: www.ncdoj.gov, Telephone: 1-919-716-6400.

If you are a resident of Massachusetts, note that pursuant to Massachusetts law, you have the right to obtain a copy of any police report.

Massachusetts law also allows consumers to request a security freeze. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. 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.

The fee for placing a security freeze on a credit report is \$5.00. If you are a victim of identity theft and submit a valid investigative report or complaint with a law enforcement agency, the fee will be waived. In all other instances, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze. If you have not been a victim of identity theft, you will need to include payment to the credit reporting agency to place, lift, or remove a security freeze by check, money order, or credit card.

If you are a resident of Oregon, you may contact the Oregon Attorney General at Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096; Email: help@oregonconsumer.gov; Telephone: 1-877-877-9392.

If you are a resident of Rhode Island, you may contact the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903; Telephone: (401) 274-4400; Website: <http://www.riag.ri.gov>. The total number of affected individuals is currently 18.

If you are a resident of New Mexico, you have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to <http://consumersunion.org/pdf/security/securityNM.pdf>

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

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com

TransUnion Security Freeze, PO Box 2000, Chester, PA 19022-2000, www.transunion.com

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 the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) 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 identity 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 (3) 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 bureaus 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 bureaus have three (3) business days after receiving your request to remove the security freeze.

If you are a resident of West Virginia, you also have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies. Contact information for each of the three credit reporting agencies is as follows:

Equifax, PO Box 740256, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-680-7289

As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file. You may choose between two types of fraud alert. An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.ftc.gov/idtheft/.

You may also obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a security freeze on your credit report pursuant to West Virginia law. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a unique personal identification number ("PIN") or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number ("PIN") or password provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. The period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request.

A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities.

If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, a few days before actually applying for new credit.