Troutman Sanders LLP
5 Park Plaza, Suite 1400
Irvine, CA 92614-2545

troutman.com

troutman sanders

Sadia Mirza
sadia.mirza@troutman.com

January 15, 2020

OVERNIGHT MAIL

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

To Whom It May Concern:

I am writing on behalf of my client, Northerner Scandinavia AB, located at Mobelgatan 4, 43133 Molndal, Sweden and which owns Northerner Scandinavia Inc., located at 6 State Rd., Mechanicsburg, Pennsylvania 17050 (collectively, "Northerner"), regarding a recent data security incident. The incident potentially impacted eight (8) New Hampshire residents. Notice of the incident will be sent to such residents via US mail on or about January 17, 2020 and a dedicated call center will be set up for consumers should they have any questions or concerns. Sample copies of such notices are attached for reference. We have also submitted notice of this incident to DOJ-CPB@doj.nh.gov.

Incident

On December 4, 2019, a Northerner employee discovered that unauthorized script was placed on the "checkout" page on one of Northerner's websites, www.nicokick.com. A similar issue was discovered on December 9, 2019 in connection with another website, www.northerner.com. The unauthorized script potentially allowed the third party that placed the script to capture information submitted by customers on the checkout pages of the websites if credit card data was entered and the "place order" button was hit. In both instances, Northerner immediately disabled the credit card payment function on the applicable site and removed the unauthorized script. Through its investigations, Northerner discovered that the unauthorized script was likely placed on the websites on or about November 30, 2019.

Potentially Impacted Information

The information potentially involved was limited to: First Name; Last Name; Street Address; City; State; Zip/Postal Code; Country; Phone Number; Email Address; Password (if this value was entered to create an account); Payment Card Number; Payment Card Security Code; Payment Card Month/Year of Expiration if the values for these items were typed into the

checkout page on the websites and the "place order" button was hit. The unauthorized script may have also captured web browser and operating system information.

Remedial Steps

Northerner immediately began an investigation as soon as it suspected a problem. Northerner also quickly contacted the Federal Bureau of Investigation and brought in a leading forensics firm to assist in the investigation. In addition, Northerner is also taking certain technical precautions in effort to prevent this type of incident from occurring again.

Should you have any questions or concerns about this matter, please do not hesitate to contact me using the contact information provided below.

Sincerely,

Sadia Mirza
Direct: 949.622.2786
sadia.mirza@troutman.com

Enclosures

Company Logo

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

NOTICE OF DATA BREACH

Dear <<Name 1>>

On behalf of Northerner Scandinavia AB, located at Mobelgatan 4, 43133 Molndal, Sweden and which owns Northerner Scandinavia Inc., located at 6 State Rd., Mechanicsburg, Pennsylvania 17050 (collectively, "**Northerner**"), we are writing to inform you about a recent incident involving the potential exposure of some of your personal information on www.nicokick.com (the "**NicoKick Website**").

WHAT HAPPENED?
On December 4, 2019, we discovered that unauthorized script was placed on the "checkout" page of the NicoKick Website. The unauthorized script potentially allowed the third party that placed the script to capture information submitted by customers on the checkout page of the NicoKick Website ***if*** credit card data was entered and the "place order" button was hit. Upon discovery of the incident, Northerner immediately disabled the credit card payment function on the site and removed the unauthorized script. Through our investigations, we discovered that the unauthorized script was likely placed on the website on or about November 30, 2019.

WHAT INFORMATION WAS INVOLVED?
The information potentially involved was limited to: First Name; Last Name; Street Address; City; State; Zip/Postal Code; Country; Phone Number; Email Address; Password (if this value was entered to create an account); Payment Card Number; Payment Card Security Code; and Payment Card Month/Year of Expiration ***if*** the values for these items were typed into the checkout page on the NicoKick Website and the "place order" button was hit. The unauthorized script may have also captured web browser and operating system information.

WHAT ARE WE DOING?
We immediately began an investigation as soon as we suspected a problem. We quickly contacted the Federal Bureau of Investigation and brought in a leading forensics firm to assist in our investigation. In addition, we are also taking certain technical precautions in effort to prevent this type of incident from occurring again.

WHAT YOU CAN DO.
1. **Monitor Account Statements and Free Credit Reports**. You should remain vigilant for incidents of financial fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports.

2. **Change Passwords.** We recommend you change your password for any online accounts, including accounts with Northerner and any other account on which you used the same or similar information used for your Northerner account.

3. **Contact the Federal Trade Commission, Law Enforcement and Credit Bureaus.** You may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's websites at www.IdentityTheft.gov and www.ftc.gov/idtheft; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

   You may contact the nationwide credit reporting agencies at:

   Equifax
   (800) 525-6285
   P.O. Box 740241
   Atlanta, GA 30374-0241
   www.equifax.com

   Experian
   (888) 397-3742
   P.O. Box 9701
   Allen, TX 75013
   www.experian.com

   TransUnion
   (800) 916-8800
   Fraud Victim Assistance Division
   P.O. Box 2000
   Chester, PA 19022
   www.transunion.com

4. **Obtain Free Copy of Credit Reports**. You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under the Fair Credit Reporting Act ("**FCRA**"), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228.

5. **Additional Rights Under the FCRA.** You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

6. **Request Fraud Alerts and Security Freezes.** You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. 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, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

   In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze at no cost to you:

Equifax	Experian	TransUnion
(800) 349-9960	(888) 397-3742	(888) 909-8872

   Placing a security freeze prohibits the agency from releasing any information about your credit report without your written authorization. Security freezes must be placed separately at each of the three nationwide credit reporting agencies. When requesting a security freeze, you may need to provide the following information:

- Your full name, with middle initial as well as Jr., Sr., II, etc.
- Social Security number
- Date of birth
- Current address and all addresses for the past two years
- Proof of current address, such as a current utility bill or telephone bill
- Legible copy of a government-issued identification card, such as a state driver's license, state identification card, or military identification.

After receiving your request, each agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

7. **Additional Information for Certain States.** Please review the last page of this letter for additional information for certain states.

FOR MORE INFORMATION

We regret any inconvenience or concern this incident may cause you. Please do not hesitate to contact our support agents for this event at <Toll Free Number> or by sending an email message to hannah.kaber@hayppgroup.com if you have any questions or concerns.

Sincerely,

Signature Image

Hannah Kaber
General Counsel

ADDITIONAL INFORMATION FOR CERTAIN STATES

For residents of Iowa: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, http://www.iowaattorneygeneral.gov/.

For residents of Maryland: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

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

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

For residents of North Carolina: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

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

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(919) 716-6400
http://www.ncdoj.com

For residents of New York: You may obtain security breach response information and identity theft and protection information from the FTC, the Department of State, Division of Consumer Protection, and the New York Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

Department of State
Division of Consumer Protection
(800) 697-1220
https://www.dos.ny.gov/consumerprotection

Office of the
Attorney General
(800) 771-7755
https://ag.ny.gov/

For residents of Rhode Island: You have the right to file or obtain a police report (should one be filed) and request a free security freeze, free of charge, as described above. Placing a security freeze may require that you provide certain personal information (*e.g.*, name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze. You may also contact the Attorney General's office at: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400, http://www.riag.ri.gov/.

For residents of Massachusetts: You have the right to obtain a police report (should one be filed) and request a free security freeze, free of charge, as described above. Placing a security freeze may require that you provide certain personal information (*e.g.*, name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze.

Company Logo

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

NOTICE OF DATA BREACH

Dear <<Name 1>>

On behalf of Northerner Scandinavia AB, located at Mobelgatan 4, 43133 Molndal, Sweden and which owns Northerner Scandinavia Inc., located at 6 State Rd., Mechanicsburg, Pennsylvania 17050 (collectively, "**Northerner**"), we are writing to inform you about a recent incident involving the potential exposure of some of your personal information on www.northerner.com (the "**Northerner Website**").

WHAT HAPPENED?
On December 9, 2019, we discovered that unauthorized script was placed on the "checkout" page of the Northerner Website. The unauthorized script potentially allowed the third party that placed the script to capture information submitted by customers on the checkout page of the Northerner Website ***if*** credit card data was entered and the "place order" button was hit. Upon discovery of the incident, Northerner immediately disabled the credit card payment function on the site and removed the unauthorized script. Through our investigations, we discovered that the unauthorized script was likely placed on the website on or about November 30, 2019.

WHAT INFORMATION WAS INVOLVED?
The information potentially involved was limited to: First Name; Last Name; Street Address; City; State; Zip/Postal Code; Country; Phone Number; Email Address; Password (if this value was entered to create an account); Payment Card Number; Payment Card Security Code; and Payment Card Month/Year of Expiration ***if*** the values for these items were typed into the checkout page on the Northerner Website and the "place order" button was hit. The unauthorized script may have also captured web browser and operating system information.

WHAT ARE WE DOING?
We immediately began an investigation as soon as we suspected a problem. We quickly contacted the Federal Bureau of Investigation and brought in a leading forensics firm to assist in our investigation. In addition, we are also taking certain technical precautions in effort to prevent this type of incident from occurring again.

WHAT YOU CAN DO.

1. **Monitor Account Statements and Free Credit Reports**. You should remain vigilant for incidents of financial fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports.

2. **Change Passwords.** We recommend you change your password for any online accounts, including accounts with Northerner and any other account on which you used the same or similar information used for your Northerner account.

3. **Contact the Federal Trade Commission, Law Enforcement and Credit Bureaus.** You may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's websites at www.IdentityTheft.gov and www.ftc.gov/idtheft; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

   You may contact the nationwide credit reporting agencies at:

   Equifax
   (800) 525-6285
   P.O. Box 740241
   Atlanta, GA 30374-0241
   www.equifax.com

   Experian
   (888) 397-3742
   P.O. Box 9701
   Allen, TX 75013
   www.experian.com

   TransUnion
   (800) 916-8800
   Fraud Victim Assistance Division
   P.O. Box 2000
   Chester, PA 19022
   www.transunion.com

4. **Obtain Free Copy of Credit Reports**. You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under the Fair Credit Reporting Act (**"FCRA"**), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228.

5. **Additional Rights Under the FCRA.** You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

6. **Request Fraud Alerts and Security Freezes.** You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. 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, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

   In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze at no cost to you:

Equifax	Experian	TransUnion
(800) 349-9960	(888) 397-3742	(888) 909-8872

   Placing a security freeze prohibits the agency from releasing any information about your credit report without your written authorization. Security freezes must be placed separately at each of the three nationwide credit reporting agencies. When requesting a security freeze, you may need to provide the following information:

- Your full name, with middle initial as well as Jr., Sr., II, etc.
- Social Security number
- Date of birth
- Current address and all addresses for the past two years
- Proof of current address, such as a current utility bill or telephone bill
- Legible copy of a government-issued identification card, such as a state driver's license, state identification card, or military identification.

After receiving your request, each agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

7. **Additional Information for Certain States.** Please review the last page of this letter for additional information for certain states.

FOR MORE INFORMATION

We regret any inconvenience or concern this incident may cause you. Please do not hesitate to contact our support agents for this event at <Insert Toll Free Number> or by sending an email message to hannah.kaber@hayppgroup.com if you have any questions or concerns.

Sincerely,

Signature Image

Hannah Kaber
General Counsel

ADDITIONAL INFORMATION FOR CERTAIN STATES

For residents of Iowa: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, http://www.iowaattorneygeneral.gov/.

For residents of Maryland: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

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

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

For residents of North Carolina: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

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

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(919) 716-6400
http://www.ncdoj.com

For residents of New York: You may obtain security breach response information and identity theft and protection information from the FTC, the Department of State, Division of Consumer Protection, and the New York Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

Department of State
Division of Consumer Protection
(800) 697-1220
https://www.dos.ny.gov/consumerprotection

Office of the
Attorney General
(800) 771-7755
https://ag.ny.gov/

For residents of Rhode Island: You have the right to file or obtain a police report (should one be filed) and request a free security freeze, free of charge, as described above. Placing a security freeze may require that you provide certain personal information (*e.g.*, name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze. You may also contact the Attorney General's office at: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, (401) 274-4400, http://www.riag.ri.gov/.

For residents of Massachusetts: You have the right to obtain a police report (should one be filed) and request a free security freeze, free of charge, as described above. Placing a security freeze may require that you provide certain personal information (*e.g.*, name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze.