

**BRANN & ISAACSON**  
ATTORNEYS AND COUNSELORS AT LAW

NATHANIEL A. BESSEY | Partner  
nbessey@brannlaw.com

September 6, 2017

RECEIVED

SEP 08 2017

CONSUMER PROTECTION

Consumer Protection and Antitrust Bureau  
Office of the Attorney General  
33 Capital Street  
Concord, NH 03301

Dear Attorney General:

This firm represents The reThink Group, Inc. of Cumming, Georgia. Pursuant to N.H. Rev. Stat. § 359-C:19 *et seq.*, we are writing to notify you of a breach of security affecting The reThink Group, Inc. which has potentially resulted in unauthorized third party access to personal data involving 2 New Hampshire residents.

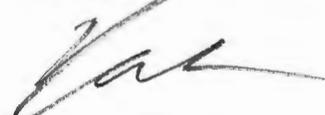
On July 11, 2017, a network intruder uploaded malicious code to The reThink Group, Inc.'s operating system, which allowed the intruder to obtain access to certain customer names, addresses, credit card numbers, CVV#s, and expiration dates entered online subsequent to that date. This breach affected only electronic information. Upon detection, the malicious code was immediately disabled by The reThink Group, Inc., and the vulnerability removed. System security was fully restored August 4, 2017.

Pursuant to New Hampshire law, potentially impacted New Hampshire residents will shortly receive written notice of such breach via U.S. Mail, which will be sent to the most recent address of record in The reThink Group, Inc.'s records. Enclosed please find a copy of the letter. The reThink Group, Inc. will be offering identity protection and restoration and credit monitoring services through Experian for a period of 12 months.

If you have any questions regarding this notification, please contact me at 207-786-3566.

Sincerely,

Brann & Isaacson



Nathaniel Bessey

## Notice of Data Breach

[Company Logo]

The reThink Group, Inc.  
5870 Charlotte Lane, Suite 300  
Cumming, GA 30040

[DATE]

Name  
Address  
Address

Dear [name]:

We are contacting you because we have learned of a data security incident that occurred between July 11, 2017 and August 4, 2017 that may have involved some of your personal information.

### *What Happened*

On July 11, a network intruder uploaded malicious code to our operating system which allowed the intruder to obtain access to certain personal information provided by customers on our websites.

### *What Information Was Involved*

The incident involved customer names, addresses, credit card numbers, CVV#,s, and expiration dates. No other information was accessed. You can learn more about the information we collect from customers by viewing our privacy policy, at <http://common.rethinkgroup.org/legal/?doc=privacy>.

### *What We Are Doing*

We take the security of our customer's personal information very seriously. Upon detection we took immediate action to disable the malicious code and prevent exposure of additional data. We continue to investigate this incident, and are implementing safeguards to prevent similar intrusions from occurring in the future.

While we have no information to indicate that your information has been or will be misused, we believe it is important that you be informed of this incident and that you take precautions to protect against possible misuse. To protect you we have retained Experian, a specialist in identity theft protection, to provide you with 12 months of its Identity Restoration service, free of charge. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration).

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to assist you (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies if necessary).

Additionally, you may activate the fraud detection tools available through Experian IdentityWorks<sup>SM</sup> as a complimentary twelve month membership by following the steps below:

- Ensure that you **enroll by**: November 30, 2017 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://experianidworks.com/creditone>
- Provide your **activation code**: [code]; and your engagement number XXXXXX.

If you have questions, please contact Experian's customer care team at 877-890-9332 by November 30, 2017. A credit card is not required for enrollment in Experian IdentityWorks. Once enrolled, you will have access to:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

\* Offline members will be eligible to call for additional reports quarterly after enrolling

\*\* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

#### *What You Can Do*

As a precautionary step, we recommend that you immediately place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. To do so, call any one of the three major credit bureaus listed below. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts.

Equifax  
1-800-525-6285  
P.O. Box 740256  
Atlanta, GA 30374

Experian  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013

TransUnionCorp  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000

You can also obtain a free credit report from each by calling 1-877-322-8228 or by logging onto [www.annualcreditreport.com](http://www.annualcreditreport.com).

#### *More Information*

We recommend you closely monitor your financial accounts and, if you see any unauthorized activity, promptly contact your financial institution and local law enforcement or your state's attorney general.

**For Maryland residents,** you may contact the Attorney General at the following address: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (410) 576-6300 or 1 (888) 743-0023 toll-free in Maryland.

**For North Carolina residents,** you may contact the Attorney General at the following address: Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, Telephone: (919) 716-6400, Fax: (919) 716-6750.

You may submit a complaint with the Federal Trade Commission by calling 1-877-ID-THEFT (1-877-438-4338) or online at <https://www.ftccomplaintassistant.gov/>, or by writing to the Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically.

We regret that your information may have been subject to unauthorized access. The reThink Group, Inc. is committed to maintaining the privacy of your information and takes many precautions for the security of personal information. The reThink Group, Inc. is continually improving its systems and practices to enhance the security of sensitive information. We sincerely regret any inconvenience this incident presents to you.

Sincerely,

Reggie Goodin  
Chief Operating and Financial Officer  
The reThink Group, Inc.