

LINN F. FREEDMAN

One Financial Plaza, Suite 1430
Providence, RI 02903-2485
Main (401) 709-3300
Fax (401) 709-3399
lfreedman@rc.com
Direct (401) 709-3353

RECEIVED

MAR 02 2020

CONSUMER PROTECTION

Also admitted in Massachusetts

Sent via *First-Class Mail*

February 27, 2020

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Breach Notification

Dear Attorney General MacDonald:

Please be advised that we represent RailWorks Corporation (“RailWorks”) regarding a recent security incident. Pursuant to RSA § 359-C:20, we are reporting to you, on behalf of RailWorks, that RailWorks notified seven (7) New Hampshire residents of a breach of their personal information.

On January 27, 2020, RailWorks was the victim of a sophisticated cyberattack in which an unauthorized third-party encrypted its servers and systems that contained personal information of RailWorks’ employees, former employees, current and former employees’ beneficiaries/dependents and/or some independent contractors. The personal information potentially accessed as a result of this cyberattack may have included names, addresses, Social Security numbers, driver’s license numbers and/or government issued IDs, dates of birth and/or dates of hire/termination and/or retirement, as applicable.

The New Hampshire residents affected by this incident will receive the enclosed notice on or about February 27, 2020 pursuant to RSA § 359-C:20. RailWorks is offering the affected individuals credit monitoring at no charge for a period of twelve (12) months.

If you have any questions, please do not hesitate to contact me.

Sincerely,



Linn F. Freedman

Enclosures



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

<<Date>>

RE: NOTICE OF A DATA BREACH

Dear <<Name 1>>:

RailWorks Corporation (“RailWorks”) is committed to protecting the confidentiality of our former employees’, employees’, former employees’ beneficiaries and dependents, and independent contractors’ information.

WHAT HAPPENED? WHAT INFORMATION WAS INVOLVED?

RailWorks was the victim of a sophisticated cyberattack in which an unauthorized third party encrypted its servers and systems, which may have involved access to your name, address, Social Security number, date of birth and date of hire/termination and/or retirement.

WHAT WE ARE DOING.

While we have no indication that any of your personal information has been misused, we are taking precautionary measures to help you protect your financial security and help to alleviate any concerns you may have.

We are committed to helping those who may have been impacted by this unfortunate situation. That’s why we are providing you with access to free credit monitoring for twelve (12) months through Identity Guard® Total.

Identity Guard® Total provides essential monitoring and protection of not only credit data, but also monitors the Dark Web and alerts you if your Social Security number, credit cards, and bank account numbers are found in unsecure online locations.

IDENTITY GUARD® TOTAL features include:

- Dark Web Monitoring
- IBM Watson® Artificial Intelligence
- High Risk Transaction Alerts
- U.S.-Based Identity Theft Recovery Assistance
- 3-Bureau Credit Monitoring
- \$1 Million Identity Theft Insurance
- Account Access via Mobile App
- Anti-Phishing App
- PC Protection Tools

For more information on these services, please call 866-977-1068 between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday, and provide your name and email address to the representative. Upon provision of your email address, you will receive additional instructions for enrollment via email at the email address provided within thirty (30) days.

In order to enroll, you will need to provide the following personal information to Identity Guard®:

- Mailing Address
- Phone Number
- Social Security Number
- Date of Birth
- E-mail Address

WHAT YOU CAN DO.

If you choose not to use these services, **we strongly urge you to do the following:**

If you choose to place a fraud alert or security freeze on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

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. There is no charge to request a credit freeze.

In order to request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five (5) years;
- Proof of current address such as a current utility bill or telephone bill; and
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.).

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 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 (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.

Should you wish to obtain a credit report and monitor it on your own, you may obtain free copies of your credit report by visiting www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.) Upon receipt of your credit report, we recommend that you review it carefully for any suspicious activity.

OTHER IMPORTANT INFORMATION.

You can also obtain more information about identity theft and ways to protect yourself from the Federal Trade Commission (FTC). The FTC has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft.

For more information about identity theft and your tax records, we recommend that you visit the IRS Taxpayer Guide to Identity Theft at <http://www.irs.gov>. You may want to consider notifying the IRS that your tax records may be at risk by completing IRS Form 14039 (Identity Theft Affidavit) which can be located at <http://www.irs.gov/pub/irs-pdf/f14039.pdf>. You will need to send Form 14039 to the IRS along with a copy of your valid government-issued identification, such as a Social Security card, driver's license, or passport to the address on the form or by faxing to 1-855-807-5720.

Detailed below are a few things to keep in mind when filing Internal Revenue Service Form 14039:

- All documents, including your identification, must be clear and legible;
- The identity theft marker will remain on your file for a minimum of three tax cycles;
- Any returns containing your Social Security number will be reviewed by the IRS for possible fraud; and
- The marker may delay the processing of any legitimate tax returns.

You may also review your rights under the federal Fair Credit Reporting Act, which can be found at <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

If you are an Iowa resident, you may also report suspected incidents of identity theft to local law enforcement or the Iowa Attorney General, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319-0106, or via telephone or email at 888-777-4590 and consumer@ag.iowa.gov.

If you are a Maryland resident, you may also contact the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, at 410-576-6491, or at idtheft@oag.state.md.us to obtain more information and steps to avoid identity theft.

If you are a North Carolina resident, you may also wish to contact the North Carolina Attorney General's Office, Consumer Protection Division, at (919) 716-6000, 9001 Mail Service Center, Raleigh, NC 27699-9001, or by visiting <http://www.ncdoj.gov/Home/ContactNCDOJ.aspx>.

If you are a New York resident, you may also wish to contact the New York Attorney General's Office, Consumer Protection Division by telephone at 800-697-1220 or at <https://www.dos.ny.gov/consumerprotection/>.

If you are an Oregon resident, you may also contact the Oregon Attorney General, Consumer Division, at 1-877-877-9392 or help@oregonconsumer.gov. You may also choose to report any incidents of identity theft or fraud to your local law enforcement.

Remember to remain vigilant in reviewing your account statements, monitoring your free credit reports, and for incidents of fraud or identity theft.

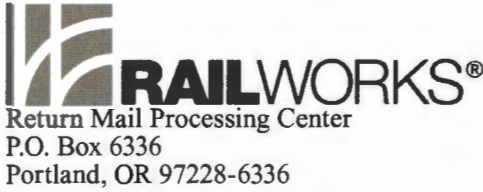
FOR MORE INFORMATION.

We regret any inconvenience this may cause you. If you have any questions please do not hesitate to contact us at 866-977-1068 between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday.

Sincerely,



Harry Glantz, Sr. VP of HR



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

<<Date>>

RE: NOTICE OF A DATA BREACH

Dear <<Name 1>>:

RailWorks Corporation (“RailWorks”) is committed to protecting the confidentiality of our employees’ information. In follow-up to the email notifications you received on January 30, 2020, and February 7, 2020, we provide you with this notice as required by applicable law.

WHAT HAPPENED? WHAT INFORMATION WAS INVOLVED?

As you know, RailWorks was the victim of a sophisticated cyberattack in which an unauthorized third party encrypted its servers and systems, which may have involved access to your name, address, driver’s license number and/or government issued ID, Social Security number, date of birth and date of hire/termination and/or retirement.

WHAT WE ARE DOING.

While we have no indication that any of your personal information has been misused, we are taking precautionary measures to help you protect your financial security and help to alleviate any concerns you may have.

We are committed to helping those who may have been impacted by this unfortunate situation. That’s why we are providing you with access to free credit monitoring for twelve (12) months through Identity Guard® Total.

Identity Guard® Total provides essential monitoring and protection of not only credit data, but also monitors the Dark Web and alerts you if your Social Security number, credit cards, and bank account numbers are found in unsecure online locations.

Enrollment is quick and easy—online or over the phone, simply follow the enrollment procedures below.

IDENTITY GUARD® TOTAL features include:

- Dark Web Monitoring
- IBM Watson® Artificial Intelligence
- High Risk Transaction Alerts
- U.S.-Based Identity Theft Recovery Assistance
- 3-Bureau Credit Monitoring
- \$1 Million Identity Theft Insurance
- Account Access via Mobile App
- Anti-Phishing App
- PC Protection Tools

All employees also have the option to buy up in coverage as the Premier coverage tier is still available and will require a payment method during your enrollment.

In order to enroll, you will need to provide the following personal information:

- Mailing Address
- Phone Number
- Social Security Number
- Date of Birth
- Email Address

Note: You must enter your first and last name exactly as it appears in RailWorks Corporation's system or you may not pass the eligibility check.

ENROLLMENT PROCEDURE for UNION Employees:

Go to the below link to activate your coverage or call Customer Service at 1-855-443-7748.

<https://app.identityguard.com/eligibility/railworksunion>

ENROLLMENT PROCEDURE for NON-UNION Employees:

If you are **currently not enrolled** in Identity Guard **or need to change your coverage:**

- Go to the below link to activate your coverage or call Customer Service at 1-855-443-7748.

<https://app.identityguard.com/eligibility/railworks1>

If you are **currently enrolled in the Individual Value Plan:**

- Your plan coverage *automatically transferred* to Total Individual *effective February 25, 2020.*

However, if you would like for your Total Individual coverage to be effective immediately *or* you need to change your coverage from Individual to Family you must contact customer service (1-855-443-7748) to cancel your current plan and enroll in either the Total Individual or Total Family coverage.

If you are **currently enrolled in the Individual Total Plan or Family Total Plan:**

- Due to your account settings containing your current payment method, Identity Guard is unable to remove your protected payment method and you will need to reenroll in this plan. You will receive an email from Identity Guard indicating your current plan is canceled. Please use the below link to reenroll in coverage or call Customer Service at 1-855-443-7748.

<https://app.identityguard.com/eligibility/railworks1>

If you are **currently enrolled in the Individual Premier Plan or Family Premier Plan:**

- Your current election remains unaffected and there is no action required.

If you experience any issue throughout the enrollment process, please contact the RailWorks HR Department at RWKSHR@railworks.com.

WHAT YOU CAN DO.

If you choose not to use these services, **we strongly urge you to do the following:**

If you choose to place a fraud alert or security freeze on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

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. There is no charge to request a credit freeze.

In order to request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five (5) years;
- Proof of current address such as a current utility bill or telephone bill; and
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.).

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 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 (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.

Should you wish to obtain a credit report and monitor it on your own, you may obtain free copies of your credit report by visiting www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.) Upon receipt of your credit report, we recommend that you review it carefully for any suspicious activity.

OTHER IMPORTANT INFORMATION.

You can also obtain more information about identity theft and ways to protect yourself from the Federal Trade Commission (FTC). The FTC has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft.

For more information about identity theft and your tax records, we recommend that you visit the IRS Taxpayer Guide to Identity Theft at <http://www.irs.gov>. You may want to consider notifying the IRS that your tax records may be at risk by completing IRS Form 14039 (Identity Theft Affidavit) which can be located at <http://www.irs.gov/pub/irs-pdf/f14039.pdf>. You will need to send Form 14039 to the IRS along with a copy of your valid government-issued identification, such as a Social Security card, driver's license, or passport to the address on the form or by faxing to 1-855-807-5720.

Detailed below are a few things to keep in mind when filing Internal Revenue Service Form 14039:

- All documents, including your identification, must be clear and legible;
- The identity theft marker will remain on your file for a minimum of three tax cycles;
- Any returns containing your Social Security number will be reviewed by the IRS for possible fraud; and
- The marker may delay the processing of any legitimate tax returns.

You may also review your rights under the federal Fair Credit Reporting Act, which can be found at <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

If you are an Iowa resident, you may also report suspected incidents of identity theft to local law enforcement or the Iowa Attorney General, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319-0106, or via telephone or email at 888-777-4590 and consumer@ag.iowa.gov.

If you are a Maryland resident, you may also contact the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, at 410-576-6491, or at idtheft@oag.state.md.us to obtain more information and steps to avoid identity theft.

If you are a North Carolina resident, you may also wish to contact the North Carolina Attorney General's Office, Consumer Protection Division, at (919) 716-6000, 9001 Mail Service Center, Raleigh, NC 27699-9001, or by visiting <http://www.ncdoj.gov/Home/ContactNCDOJ.aspx>.

If you are a New York resident, you may also wish to contact the New York Attorney General's Office, Consumer Protection Division by telephone at 800-697-1220 or at <https://www.dos.ny.gov/consumerprotection/>.

If you are an Oregon resident, you may also contact the Oregon Attorney General, Consumer Division, at 1-877-877-9392 or help@oregonconsumer.gov. You may also choose to report any incidents of identity theft or fraud to your local law enforcement.

Remember to remain vigilant in reviewing your account statements, monitoring your free credit reports, and for incidents of fraud or identity theft.

FOR MORE INFORMATION.

We regret any inconvenience this may cause you. If you have any questions please do not hesitate to contact us at 866-977-1068 between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday.

Sincerely,

A handwritten signature in black ink, appearing to read "Harry Glantz", with a stylized flourish at the end.

Harry Glantz, Sr. VP of HR