

Robert L. Kardell

1700 Farnam Street
Suite 1500
Omaha, NE 68102-2068
Tel: 402.344.0500
Fax: 402.344.0588
Direct: 402.636.8313
bkardell@bairdholm.com
www.bairdholm.com

February 15, 2023

CONFIDENTIAL
VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Data Breach
Client-Matter No. DRT, LLC, D0129- 00053

To Whom It May Concern:

Our firm represents DRT, LLC ("DRT") in Carter Lake, Iowa. DRT recently experienced a data breach, and the purpose of this letter is to provide notification of the data breach pursuant to the Maryland Personal Information Protection Act, MD Code, Commercial Law, § 14-3504(h).

IDENTIFICATION OF PARTIES

DRT is a shared services company located at 2200 Abbott Drive, Carter Lake, IA 51510. DRT's contact person is Aaron Gunderson, General Counsel, (712) 248-7027.

NATURE OF THE BREACH

On January 19, 2023, DRT discovered unauthorized remote access to a DRT owned computer that occurred on January 18, 2023. After learning of the incident, DRT immediately hired a third-party computer security firm to conduct an investigation and to identify any personally identifiable information (PII) which may have been compromised. Although the investigation could not determine whether any information was accessed, acquired, or misused, it is possible that there was unauthorized access or acquisition to PII in files saved to the computer, such as a spreadsheet or documents used for internal business purposes.

DRT manually reviewed the contents of the computer and determined that the information that may have been accessed included consumers' full names and demographic information (such as address, city, state, and zip code), and Social Security number.

NUMBER OF RESIDENTS AFFECTED

The total number of impacted individuals is approximately 7,857 individuals, including 131 Maryland residents. DRT will mail breach notification letters to impacted individuals on February 17, 2023. A template copy of the notice to impacted individuals is included with this letter.

STEPS TAKEN IN RESPONSE TO THE INCIDENT

After learning of the incident, DRT took a number of important steps to prevent similar incidents from occurring in the future. This included isolating the device from DRT's network and the internet, temporarily disabling the user's account while a password reset was performed, revoking all active user logins as well as any multi-factor authentication and monitoring the user's activity within DRT's on-premises and cloud-based environments. DRT is also working to implement additional technologies designed to prevent similar attacks including upgrading software to deploy additional computer activity analysis applications which will provide real-time alerts and monitoring. DRT will also be providing expanded cybersecurity training for its employees.

CREDIT MONITORING SERVICES

As a safeguard, DRT has arranged for impacted individuals to enroll, at no cost, in an online credit monitoring service for twenty-four (24) months provided by IDX. Impacted individuals can sign up for the online or offline credit monitoring service any time between February 17, 2023 and May 18, 2023. Once enrolled, impacted individuals are able to obtain services including: credit monitoring service with notifications of any critical changes to the individual's credit history, fraud alerts, credit inquiries, new accounts, new public records, late payments, changes of address, and an identity restoration program that provides assistance in the event that an individual's identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible (policy exclusions may apply).

In addition, the breach notification letters include information about other precautionary measures, including obtaining free credit reports and placing a fraud alert and/or security freeze on credit files.

CONTACT INFORMATION

If you have any questions regarding this notification, please contact me at (402) 636-8313 or bkardell@bairdholm.com.

Sincerely,



Robert L. Kardell
FOR THE FIRM
Baird Holm LLP

BLK/BLK
Attachment



P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-753-7056
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

February 17, 2023

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

What Happened

DRT, LLC (“DRT”) recently experienced a cybersecurity incident that involves some of your personally identifiable information (“PII”). On January 19, 2023, we discovered unauthorized remote access to a DRT owned computer that occurred on January 18, 2023. After learning of the incident, DRT immediately hired a third-party computer security firm to conduct an investigation and to identify any PII which may have been compromised. Although that the investigation could not determine whether any information was accessed, acquired or misused, it is possible that there was unauthorized access or acquisition to PII in files saved to the computer, such as a spreadsheet or documents used for internal business purposes. DRT is providing this notice so that you can take steps to protect against possible misuse of personal information.

What Information Was Involved

DRT manually reviewed the contents of the computer, including all files located on the computer, to determine the type of PII potentially involved. Our investigation indicated that some of your information was on the affected computer. Information that may have been accessed or acquired includes full name and demographic information (such as address, city, state, and zip code) <<Variable Data 2>> and your Social Security number.

What We Are Doing

After learning of the incident, DRT took a number of important steps to prevent similar incidents from occurring in the future. This included isolating the device from our network and the internet, temporarily disabling the user’s account while a password reset was performed, revoking all active user logins as well as any multi-factor authentication and monitoring the user’s activity within our on-premises and cloud-based environments. DRT is also working to implement additional technologies designed to prevent similar attacks including upgrading our software to deploy additional computer activity analysis applications which will provide real-time alerts and monitoring. DRT will also be providing expanded cybersecurity training for its employees.

We are offering complimentary identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity theft protection services by calling 1-833-753-7056 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is May 17, 2023.

We encourage you to take advantage of this service offering. IDX representatives can answer questions or concerns you may have regarding this incident and steps to protect your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-753-7056 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in cursive script that reads "Hanna Heit". The signature is written in dark ink and is positioned above a thin horizontal line.

Chief Manager
DRT, LLC

(Enclosure)



Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-753-7056 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Additional Privacy Safeguard Information.

For Iowa Residents:

Residents of Iowa may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft at the following:

Office of the Attorney General of Iowa
Director of Consumer Protection Division
Hoover State Office Building
1305 E. Walnut Street, Des Moines, IA 50319
1-515-281-5926 / 888-777-4590 (outside of Des Moines metro area, Iowa only)
www.iowaattorneygeneral.gov

For Maryland Residents:

Residents of Maryland can contact the State of Maryland Attorney General's Office for more information about steps an individual can take to avoid identity theft using the following:

Toll Free: 1-888-743-0023
Phone: (410) 576-6491
Fax: (410) 576-6566
E-mail: idtheft@oag.state.md.us
Mail: 200 St. Paul Place, 25th Floor, Baltimore, MD 21202
ID Theft Web Site: <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>

For Massachusetts Residents:

Residents of Massachusetts have the right to obtain a police report regarding this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New York Residents:

Residents of New York may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755
www.ag.ny.gov

For North Carolina Residents:

Residents of North Carolina can contact the State of North Carolina Attorney General's Office for more information about steps an individual can take to avoid identity theft using the following:

Toll Free: 1-877-5-NO-SCAM (1-877-566-7226)

Phone: (919) 716-6000

Mail: 9001 Mail Service Center, Raleigh, NC 27699-9001

Online Contact Form: <https://ncdoj.gov/contact-doj/>

ID Theft Web Site: <https://ncdoj.gov/protecting-consumers/protecting-your-identity/>

For New Mexico Residents:

Under the Fair Credit Reporting Act you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

For Oregon Residents:

Oregon Residents should report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows:

Oregon Department of Justice

1162 Court Street NE

Salem, OR 97301

1-877-877-9392

www.doj.state.or.us

Fraud Alert Information

Whether or not you enroll in credit monitoring, we recommend that you place a "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. The contact information for the three nationwide credit reporting companies is:

Equifax

PO Box 740256

Atlanta, GA 30374

www.equifax.com

1-800-525-6285

TransUnion

PO Box 2000

Chester, PA 19016

www.transunion.com/fraud

1-800-680-7289

Experian

PO Box 9554

Allen, TX 75013

www.experian.com

1-888-397-3742

Free Credit Report Information

Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

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. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report or notify your state's Attorney General Office. Attorney General Office contact information for each and every state and U.S. Territory can be found at <https://www.naag.org/find-my-ag/>.

Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the **Federal Trade Commission (FTC)** at www.identitytheft.gov or at **1-877-ID-THEFT (1-877-438-4338)**. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. Also visit the FTC's website at www.ftc.gov/idtheft to review their free identity theft resources such as their comprehensive step-by-step guide "Identity Theft - A Recovery Plan".

Security Freeze Information

You can request a "Security Freeze" on your credit file by sending either, (i) a request in writing, by mail, to each of the three nationwide credit reporting companies, or (ii) via the Internet at the credit reporting companies' websites listed below. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. The Security Freeze may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report. This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions and extension of credit at point of sale.

To place a Security Freeze on your credit files at all three nationwide credit reporting companies, write to the addresses below or visit each of the credit reporting company websites listed below for information on Security Freeze services:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com>
1-800-685-1111

TransUnion Security Freeze
PO Box 2000
Chester, PA 19016
<http://transunion.com/freeze>
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

The consumer credit reporting company will provide you with a personal identification number (PIN) or password to use if/when you choose to remove the freeze on your consumer credit report or to authorize the release of your consumer credit report to a specific party or for a specified period of time after the freeze is in place.