



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

23439



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

<<Date>>

**NOTICE OF DATA BREACH**

Re: **Important Security Notification**  
**Please read this letter.**

Dear <<Name 1>>:

We are contacting you regarding a security incident that may have involved some of your personal information. We take the privacy and security of your personal information very seriously and for this reason want you to understand the steps we have taken to address this issue and additional steps you can take to protect yourself. This letter explains what happened and, as a precaution, offers you additional assistance in protecting against potential identity theft. As further described in this letter, we are offering you complimentary credit monitoring and identity theft restoration services.

**What Happened**

On August 26, 2021, we determined that our computer network was affected by a data security incident. We immediately began an investigation to assess the incident's scope and engaged a third-party cybersecurity firm to assist with that investigation. We preemptively shut down select systems to contain the incident and then undertook a secure, managed restoration of those systems. In addition, we promptly notified law enforcement and have been cooperating with their investigation of the incident. Based on the investigation, we have determined that the earliest indication of unauthorized activity was on August 18, 2021, and the last indication of activity was on August 26, 2021.

**What Information Was Involved**

Based on the investigation, we have assessed that some of your personal information was in files that may have been accessed without authorization. Depending on the document(s), this information may have included your name and the following: <<Data Elements>>.

**What We Are Doing**

We preemptively shut down select systems to contain the incident and then undertook a secure, managed restoration of those systems. We also engaged a third-party cybersecurity firm to assist with our review and notified law enforcement and continue to cooperate with them. We have taken steps to further strengthen and enhance the security of systems in our network, including updating administrative and technical safeguards.

**What You Can Do**

As a precaution, we are offering you a complimentary two-year membership of Equifax's Complete™ Premier membership, which provides identity theft detection and assistance in resolving any identity theft that does occur. We strongly recommend you take advantage of this offer.

<sup>1</sup> KMT Brrr! is now part of the Americold family.

To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by <<Enrollment Deadline>> (Your code will not work after this date.)
- Visit the Equifax website to enroll: <https://www.equifax.com/activate>
- Enter your unique Activation Code of <<Activation Code>> then click "Submit" and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click "Continue".

*If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.*

*Once you have successfully signed in, you will skip to the Checkout Page in Step 4.*

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click "Sign Me Up" to finish enrolling.

**You're done!**

The confirmation page shows your completed enrollment.

Click "View My Product" to access the product features.

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Equifax's Complete™ Premier online membership, please contact Equifax's customer care team at (866) 243-0734 by <<Enrollment Deadline>>.

**Additional details regarding your two-year Equifax Complete™ Premiere Membership:**

A credit card is **not** required for enrollment in Equifax's Complete™ Premier. You can contact Equifax **immediately** regarding any fraud issues, and have access to the following features once you enroll in Equifax's Complete™ Premier:

- Annual access to your 3-bureau credit report and VantageScore<sup>2</sup> credit scores.
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score.
- 3-bureau credit monitoring<sup>3</sup> with email notifications of key changes to your credit reports.
- WebScan notifications<sup>4</sup> when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites.
- Automatic fraud alerts<sup>5</sup>, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock.<sup>6</sup>
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf.
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft.<sup>7</sup>
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

<sup>2</sup> The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

<sup>3</sup> Credit monitoring from Experian and TransUnion will take several days to begin.

<sup>4</sup> WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

<sup>5</sup> The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

<sup>6</sup> Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit [www.optoutprescreen.com](http://www.optoutprescreen.com).

<sup>7</sup> The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

**More Information**

Security, in all its forms, remains a top priority at KMT Brrr!, and we will continue to take all appropriate steps to safeguard personal information and our systems. We sincerely apologize for any inconvenience or concern this incident may cause. If you have any questions regarding this incident, please call (855) 675-3090 from 9:00AM – 9:00PM EST Monday through Friday.

Sincerely,

The KMT Brrr! Team

## Reference Guide

### Order Your Free Credit Report

To order your free annual credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at [www.ftc.gov](http://www.ftc.gov) and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus (Equifax, Experian and TransUnion) provide free annual credit reports only through the website, toll-free number or request form.

You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax  
[www.equifax.com](http://www.equifax.com)  
(800) 685-1111

Experian  
[www.experian.com](http://www.experian.com)  
(888) 397-3742

TransUnion  
[www.transunion.com](http://www.transunion.com)  
(800) 916-8800

Upon receiving your credit report, review it carefully. Errors may be a warning sign of possible identity theft. Here are a few tips of what to look for:

- Look for accounts you did not open.
- Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case.
- Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

### How to Enroll in Free Credit Monitoring and Equifax's Complete™ Premier

We encourage you to contact Equifax with any questions at (866) 243-0734 and to enroll in free Complete™ Premier services by going to <https://www.equifax.com/activate> and using the Activation Code provided above. Please note that the deadline to enroll is <<Enrollment Deadline>>.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidence of identity theft or fraud, promptly report the matter to your local law enforcement authorities (from whom you can obtain a police report), state Attorney General, and the Federal Trade Commission (FTC). You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission  
Bureau of Consumer Protection  
600 Pennsylvania Avenue NW  
Washington, DC 20580  
(877) IDTHEFT (438-4338)  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

### Placing a Security Freeze

You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

You can place, temporarily lift, or permanently remove a security freeze on your credit report online, by phone, or by mail. You will need to provide certain personal information, such as address, date of birth, and Social Security number to request a security freeze and may be provided 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. Information on how to place a security freeze with the credit reporting agencies is also contained in the links below:

<https://www.equifax.com/personal/credit-report-services/>

<https://www.experian.com/freeze/center.html>

<https://www.transunion.com/credit-freeze>

Fees associated with placing, temporarily lifting, or permanently removing a security freeze no longer apply at nationwide consumer reporting agencies.

### **Placing a Fraud Alert**

To protect yourself from possible identity theft, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. You may obtain additional information from the FTC and the credit reporting agencies listed above about placing a fraud alert and/or security freeze on your credit report.

### **MARYLAND RESIDENTS**

You may obtain information about avoiding identity theft at:

Office of the State of Maryland Attorney General  
200 St. Paul Place  
Baltimore, MD 21202  
1-888-743-0023  
[www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov)

### **NORTH CAROLINA RESIDENTS**

You may obtain information about avoiding identity theft at:

North Carolina Attorney General's Office  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
919-716-6400  
[www.ncdoj.gov](http://www.ncdoj.gov)

November 3, 2021

BY ONLINE PORTAL

Massachusetts Office of the Attorney General  
Consumer Protection Division  
Attn: Data Breach Notification  
One Ashburton Place  
Boston, MA 02108

Re: Data Security Incident

Dear Attorney General Healey,

As outside counsel for Americold Realty Trust, a publicly traded REIT focused on the ownership, operation, acquisition, and development of temperature-controlled warehouses, we write to inform you of the discovery of a data security incident at an entity that Americold recently acquired -- KMT Brrr!<sup>1</sup> -- and write to explain the steps that have been taken to address the incident, including notifying potentially impacted individuals and providing them ways with which to protect their personal information.<sup>2</sup>

On August 26, 2021, KMT Brrr!, which operates two temperature-controlled facilities in New Jersey, determined that its computer network had been affected by a ransomware incident. Americold and KMT Brrr! immediately began an investigation to assess the incident's scope, including engaging a third-party cybersecurity firm at the direction of counsel to assist with the response. As a containment measure, the company preemptively shut down select systems and then undertook a secure, managed restoration of those systems. The company also promptly notified law enforcement and has been cooperating with their investigation of the incident. In addition, the company has taken steps to further strengthen and enhance the security of systems in its network, including updating administrative and technical safeguards. The company did not pay a ransom. Based on the investigation, the company

---

<sup>1</sup> Americold acquired KMT Brrr! on May 5, 2021 and is in the process of completing the integration of the company. Americold's corporate headquarters are located at 10 Glenlake Parkway, Suite 600, South Tower, Atlanta, GA 30328. KMT Brrr! is located at 1145 Commerce Boulevard, Logan, NJ 08085.

<sup>2</sup> This incident is unrelated to the one that Americold reported to this Office on about March 4, 2021.

determined that the earliest indication of unauthorized activity was on August 18, 2021, and the last indication of activity was on August 26, 2021.

Since discovering the incident, the company diligently has worked to complete its review of the potentially affected data, engaging external support to assist with the review and locating up-to-date address information for identified individuals. The review and address look up process was completed on about October 20, 2021, with the company's finding personal information for 147 state residents in files that may have been accessed or acquired without authorization. The statutorily-defined personal information involved government-issued identification information.

The company is notifying this Office and the individual state residents and is providing them with complimentary credit monitoring and identify theft services for 24 months through Equifax. An unaddressed copy of the letter template is attached.<sup>3</sup> The letters are to be mailed on November 4. In addition, the company has established a call center to answer recipient's questions.

Please do not hesitate to contact us if you have any questions regarding this letter.

Very truly yours,



Scott Ferber  
202-756-8988

Attachments

---

<sup>3</sup> The letters to the individuals are being sent on KMT Brrr! letterhead to avoid confusion by the recipients as to the incident's origin. They likely would not understand or recognize a connection to Americold.