



Storopack, Inc.
4758 Devitt Drive
Cincinnati, OH 45246
Phone (513) 874-0314

30227

June 28, 2023



Notice of Business Ransomware Security Breach

Dear 

We are writing to inform you about a data security incident that might have exposed some of your personal information. We at Storopack take the protection and proper use of your information very seriously. For this reason, we are contacting you to discuss the circumstances of the incident.

What happened?

On March 21, Storopack's parent corporation, Storopack Hans Reichenecker GmbH ("Storopack GmbH"), suffered a ransomware attack in Germany in which the company's application servers and domain controllers were encrypted and the attacker(s) demanded payment of a ransom in exchange for decryption the disabled systems. Instead of communicating with the attacker(s), Storopack disconnected all servers, network components and related PCs in order to investigate the attack and prevent any further effects upon Storopack-related systems.

Storopack GmbH immediately informed the German Police and Data Protection Authority, and has posted announcements and updates of the situation on corporate websites. Storopack GmbH also distributed to all employees a memorandum describing the incident on April 20, 2023.

What information was involved?

Storopack has not received any additional demands, threats or other communications from the attacker(s), beyond the initial encryption of systems and demand for ransomware in exchange for decryption of systems. However, this month a claim has been made on the internet that the incident did include taking of personal information.

Our investigation of the systems since the incident has not identified any specific data or other files that were accessed or stolen during the incident. However, some of the systems did contain files that included personal information for employees, such as name or address in combination with a telephone number, social security number, driver's license number, bank account number, credit or debit card number, or signature. So we are writing to you as a precaution because we do take the protection and proper use of everyone's personal information very seriously.

What we are doing?

After disconnecting the entire network, we have introduced a completely new Server environment and enhanced Security Operations Center, with additional security management and training. We are continuing to investigate the situation and cooperate with law enforcement.

We also are offering you a complimentary two year membership in the Equifax "Complete Premier" credit monitoring and identity theft protection package. This membership is completely free to you. It will not hurt your credit score. To obtain these benefits, you must enroll in the program using a unique activation code and the procedure described on the attached EQUIFAX enrollment page. We cannot enroll you in this program, so please take the additional steps set forth on the following page if you wish to participate in the program.

What can you do?

The FBI has recommended the following steps to help protect against falsified payment instructions or other attempts to exploit business email contacts:

- Be careful with what information you share online or on social media. By openly sharing things like pet names, schools you attended, links to family members, and your birthday, you can give a scammer all the information they need to guess your password or answer your security questions.
- Don't click on anything in an unsolicited email or text message asking you to update or verify account information. Look up the company's phone number on your own (don't use the one a potential scammer is providing), and call the company to ask if the request is legitimate.
- Carefully examine the email address, URL, and spelling used in any correspondence. Scammers use slight differences to trick your eye and gain your trust.
- Be careful what you download. Never open an email attachment from someone you don't know, and be wary of email attachments forwarded to you.
- Set up two-factor (or multi-factor) authentication on any account that allows it, and never disable it.
- Verify payment and purchase requests in person if possible or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.
- Be especially wary if the requestor is pressing you to act quickly.

<https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise>

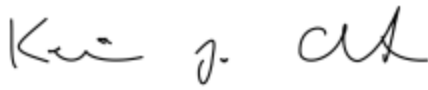
We also are enclosing an "Additional Resources" section with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please contact:

Ingo Seimetz
Data Protection Officer Storopack Group
ITEMCON Sagl
Via Balestra 12
CH-6900 Lugano
Tel. +41(91)2085199 (Please leave a message for a callback)
storopack.dpo@itemcon.com

Sincerely,



Kevin Cheek
Vice President of Human Resources
Storopack, Inc., AKA Storopack North America
4758 Devitt Dr.
Cincinnati, OH 45246

Enter your Activation Code: [REDACTED]
Enrollment Deadline: September 30, 2023



Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ 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 alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- 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 theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code [REDACTED] 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.

¹The 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.

²Credit monitoring from Experian and TransUnion will take several days to begin.

³WebScan 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.

⁴The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

⁵Locking 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

⁶The 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.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. You remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll-free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/ 1-877-IDTHEFT (438-4338).

Indiana residents may contact the Indiana Attorney General, <https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/> (800) 382-5516 or (317) 232-6330.

Iowa residents may contact their local police department to file a report, or the Attorney General's office at (515) 281-5926, toll free 1-888-777-4590, or email consumer@ag.iowa.gov. Additional resources are available at <https://www.iowaattorneygeneral.gov/for-consumers/general-consumer-information/identity-theft>

Maine residents may contact their local law enforcement office to file a report. The Maine Attorney General maintains additional resources at https://www.maine.gov/ag/privacy/identity_theft.shtml and may be contacted at (207) 626-8800.

Maryland residents may contact the Attorney General's Identity Theft Unit at (410) 576-6491, or by sending an e-mail to idtheft@oag.state.md.us. Additional resources are available at <https://www.marylandattorneygeneral.gov/pages/identitytheft/default.aspx>

Massachusetts residents may contact their local police department to file a report. They also may call the Attorney General's Consumer Assistance and Response Division at (617) 727-8400, or consult additional resources at <https://www.mass.gov/service-details/report-identity-theft>

New Jersey residents may contact their local police department to file a report. Additional resources are available from the New Jersey State Police, <https://www.nj.gov/lps/njsp/tech/identity.html>

New York residents may contact the Attorney General's consumer help line at 1-800-771-7755, or consult additional resources at <https://ag.ny.gov/resources/individuals/credit-lending/identity-theft> or <https://dos.nysits.acsitefactory.com/consumer-protection>

North Carolina residents may contact the Attorney General via website at <https://ncdoj.gov/contact-doj/> or consult additional resources at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>

Oregon residents may contact the Attorney General's office at 877-877-9392, or consult additional resources at <https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/>

Virginia residents may contact the Attorney General's office at 800-370-0459, or consult additional resources at <https://www.oag.state.va.us/programs-initiatives/identity-theft>

TO ALL EMPLOYEES

Metzingen, 20th April 2023

Dear employees,

On March 21, a cyber attack was perpetrated on Storopack's global IT network.

Due to the limited communication possibilities in the last weeks as well as the necessity to collect facts first, a more extensive, internal information is provided by now and with the following.

As foreseen in our IT emergency protocol, we immediately shut down our systems after we became aware of the attack on March 21, set up the predefined crisis team in Metzingen and informed the entire organization via a telephone information cascade.

On March 22, we informed the police, other responsible authorities, and our data protection officer, and gradually began to activate our SAP emergency access.

On March 23, we informed the public by means of a press release and on our websites about the incident, our continued ability to produce and deliver, as well as our limited availability by telephone and the inaccessibility of our @storopack.com e-mail addresses.

Also on March 23, we began working with IT security experts to prepare the most secure possible restart of our systems, which has already occurred in part and will continue in the coming weeks and months until normal operations are achieved.

Despite extensive forensics, it was unfortunately not possible to determine how the attack took place. What could be traced is the outflow of data, which, however, could not be specified. According to the data protection guidelines in Germany, we have to inform all employees worldwide about this in a personalized letter. This will be done in the coming weeks.

Despite the serious consequences for our operational capability, we were able to produce and deliver worldwide at all times. There are two main reasons for this: Firstly, it is our SAP emergency access and secondly, the enormous commitment, creativity and team spirit of all of you.

We already proved during the Covid-19 pandemic that we can handle a crisis very well. Now we have another proof of great team spirit and excellent resilience.

Only our online stores in Belgium, Germany and Switzerland were unavailable.

We did not contact the attackers and consequently did not pay a ransom.

Some employees have had little work in recent weeks, others enormously more. In the coming weeks, this will gradually turn around. Thank you for your flexibility in doing so!

After the recovery of our @storopack.com e-mail addresses we can assure all external addressees that there are no viruses from the attack hidden in our emails. Through elaborate forensics and the most careful cleaning we can exclude this.

To be on the safe side, please change the passwords for all portals used from your Storopack computer.

What findings remain after the cyber attack?

Our SAP emergency access was a prerequisite for orderly emergency operations. Setting up this infrastructure in the event of a potential cyber attack was very forward-looking. Many thanks and praise to our IT team for this!

From what we have learned from the police and IT security experts, this makes us a more than rare exception. For most companies that are hit by cyber attacks, production and delivery are not possible for several months.

Nevertheless, there is potential for improvement. Above all, the impact must be less in case of a future attack. We will work on this, because cyber attacks can never be completely ruled out.

We should also look at the opportunities and positive sides: The successful handling of the attack will strengthen us for the future. Our IT systems will be even better protected and the reconfirmed crisis management capability will generate additional confidence internally and externally.

In recent weeks, we have had to do without a lot of written information and systems. Therefore, we should use the unintended experience to question what we can make easier or drop entirely in the future. Please have the courage to try things out!

Storopack's stability has not been affected by the cyber attack. The economic damage is not serious according to what we know today. Our incoming orders in the weeks since the attack have been at a normal level. In addition, Storopack is on a very solid financial basis.

My parents, my sister and I would like to sincerely thank all of you for your enormous commitment, creativity and team spirit, so that we were able to keep Storopack productive and able to deliver worldwide during the last weeks!

With best regards

A handwritten signature in black ink, appearing to read 'H. Reichenecker'. The signature is written in a cursive style with a large initial 'H' and a period following it.

Hermann Reichenecker