One of our technology partners has alerted us of an employee data breach. Unfortunately, this means that some of your data has been accessed illegally, along with colleagues at your company and others that are part of the Halma Goup in the US.

This was part of a recent cyber-attack on a file transfer system called MOVEit which has affected a large number of companies globally.

I appreciate that this news will be of concern. This message sets out what it means for you, what actions you can take, and what Halma is doing in response to the attack.

What this means for you

The information that has been accessed is as follows:

- Employee ID
- Employee name
- Employee email
- Employee date of joining
- Health savings
- Bank details (bank name and account number)
- Information relating to dependents, for some not all, this includes:
    - Names
    - Date of birth
    - Address
    - Contact number
    - Email

What you should do

1, Be alert to scams.

- Be wary of emails, phone calls or text messages from unknown sources, and do not divulge any personal information, including passwords.
- Do not click on links or attachments in suspicious emails.
- If an email appears from someone you know but looks suspicious then contact that person through other means, such as a text message or phone call, to confirm it.
- Learn more about how you can keep your information safe, and spot potential threats, here.

2, Contact your bank.

- Banks have high levels of security to protect their customers and are used to dealing with cyber security issues. Contact the bank where your salary is paid into, and it will advise on any additional steps you need to take.

3, Change your passwords.

- It is good practice to regularly change your password, especially for important online services. Follow best practice:

- Make sure your password is long and strong. Include a mixture of uppercase and lowercase characters, numbers and symbols.
- Don't reuse passwords you've used on other accounts.
- Use multi-factor authentication when it's an option.
- Consider a password manager to help securely store them.
- Pick security questions only you know the answer to.

4, Additional support.

We will shortly offer all affected employees access to an online tool to help protect you from identity theft. We will contact you as soon as it is available.

In addition, the Halma IT team and its security partners are actively monitoring the web – including what is known as the Dark Web where information is often illegally shared – to assess if any data has been leaked. We will keep you informed with all relevant new information.

Who to contact

If you have any questions or receive a suspicious email, text message or phone call then please follow the steps above and report it to your local IT helpdesk.

I understand that you may want to know exactly what data of yours has been accessed. If you do, then please contact Halma.Security@halma.com and the team will get back to you as soon as possible.

Jennifer Ward

Group Talent and Communications Director

Halma

FAQs for employees

How has this happened?

A third-party software application called MOVEit, used by large number of companies globally, suffered a cyber security breach. The data breach included some data held employees of Halma companies and Halma Group.

Has Halma or my company been hacked?

No. It was a data breach of a third-party software provider that was working for Halma.

What information of mine has been compromised?

- Employee ID
- Employee name
- Employee email
- Employee date of joining
- Health savings
- Bank details (bank name and account number)

- Information relating to dependents, for some not all, this includes:
    - Relationship to employees
    - Names
    - Date of birth
    - Address
    - Contact number (Home and or Mobile)
    - Email
    - SSN
    - Gender
    - Date of Birth

Who has got my data?

The data was accessed by a cyber-criminal organisation. Given the nature of the breach, it is unclear who has access to your data at this stage.

Have my bank details been leaked?

We understand that the breach includes bank details – bank name and account number. We recommend that you inform your bank that your pay goes into. It will advise on next steps.

Do I need to change my passwords?

We are not aware that the breach included any log-in passwords. However, it is good security practice to change them regularly. Best practice is as follows:

- Make sure your password is long and strong. Include a mixture of uppercase and lowercase characters, numbers and symbols.
- Don't reuse passwords you've used on other accounts.
- Use multi-factor authentication when it's an option.
- Consider a password manager to help securely store them.
- Pick security questions only you know the answer to.

Will I start to receive unsolicited scam or spam emails?

Given the nature of the breach, it is unclear who has access to your data at present. Therefore, please remain vigilant. Do not open suspicious or unsolicited emails and do not click on suspicious website links or attachments in emails.

Will my pay be impacted this month?

No. This vulnerability was isolated to a particular piece of third-party software which has been disconnected. Our payroll provider employs robust security processes across all our services and none of their own software is affected, meaning payroll services continue to run as normal.

Will I receive a phone call from you regarding this incident and how should I respond?

Neither we nor any third-party provider will contact you by phone directly with regards to this incident. Be very cautious about anyone calling you about investigation of this incident, even if they do not refer to any of the potentially compromised information.

Who should I contact if I have a concern or if I receive suspicious or unsolicited messages?

If you have any questions or receive a suspicious email, text message or phone call then please follow the steps above and report it to your local IT helpdesk.

ANNEX I

Additional Resources for Individuals

Obtaining copies of your credit reports.

For residents of Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont*:* You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

You may also obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report, once every 12 months from each of the agencies, by contacting any one of the following national consumer reporting agencies:

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

TransUnion: www.transunion.com or 1-800-680-7289 or TransUnion LLC, P.O. Box 1000, Chester, PA 19016

Equifax: www.equifax.com or 1-800-525-6285 or Equifax Information Services LLC, P.O. Box 740241, Atlanta, GA 30374-0241

You can also order a free credit report by visiting www.annualcreditreport.com, by calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Contacting the FTC and State Attorneys General.

All U.S. Residents**:** 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).

***For Colorado residents*, you may contact the Colorado Office of the Attorney General**, Consumer Protection: 1300 Broadway, 9th Floor, Denver, CO 80203; toll-free at 1-720-508-6000, www.coag.gov.

***For Connecticut residents*, you may contact the Connecticut Office of the Attorney General**, 165 Capital Avenue, Hartford, CT 06106; toll-free at 1-860-808-5318; https://portal.ct.gov/ag

***For DC residents*, you may contact the District of Columbia Office of the Attorney General**, Consumer Protection: 400 6th Street, NW, Washington, DC 20001; toll-free at (202)-442-9828 or by email at consumer.protection@dc.gov; https://oag.dc.gov/consumer-protection.

***For Illinois residents*, you may contact the Illinois Office of the Attorney General**, Identity Theft Hotline: 100 W Randolph St., Fl. 12, Chicago, IL 60601; toll-free at 1-866-999-5630; https://www.illinoisattorneygeneral.gov/.

***For Massachusetts residents*, you may contact to Massachusetts Office of the Attorney General**, 1 Ashburton Place, Boston, MA 02108; toll-free at 1-617-727-8400; https://www.mass.gov/contact-the-attorney-generals-office

***For Maryland residents*, you may contact the Maryland Office of the Attorney General**, Consumer Protection Division: 200 St. Paul Place, 16th Flr., Baltimore, MD 21202, www.oag.state.md.us/Consumer, and toll-free at (888) 743-0023 or (410) 528-8662.

***For New York residents*, you may contact the New York Office of Attorney General**, Consumer Frauds & Protection: The Capitol, Albany, NY 12224; toll-free at 1-800-771-7755; https://ag.ny.gov/consumer-frauds/identity-theft.

***For North Carolina residents*, you may contact the North Carolina Office of the Attorney General,** Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at (877) 566-7226 or (919) 716-6000; https://ncdog.com.

***For Rhode Island residents*, you may contact the Rhode Island Office of the Attorney General**, Consumer Protection: 150 South Main Street, Providence, RI 02903; toll-free at (401) 274-4400; https://riag.ri.gov/consumerprotection.

Reporting of identity theft and completing a police report.

***For residents of Iowa**:* We recommend that you report any suspected incidents of identity theft to law enforcement or to the Attorney General, Consumer Protection Division. https://www.iowaattorneygeneral.gov/for-consumers/general-consumer-information/identity-theft

***For residents of Massachusetts**:* You have the right to obtain a police report if you are a victim of identity theft.

***For residents of Oregon**:* State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.