MESSAGE TO FORMER EMPLOYEES

Dear [Name]

One of Halma's technology partners has alerted us of a data breach. Unfortunately, this means that some of your employee data has been accessed illegally, along with former colleagues at [your company] and others that are part of the Halma Group 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. We're sorry that this happened, and for the inconvenience it causes. 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

A number of files were accessed, containing the following information in relation to you:

- Employee ID
- Employee email, which will include your name
- Health savings account contributions
- Bank details (bank name, bank ID, account number)

Information relating to dependents, for some not all dependents, includes:

- Relationship to employee
- Names
- Date of birth
- Address
- Contact number (home and or cell phone)
- Email
- Social Security Number
- Gender

Based on expert cyber security advice we have received, the most likely risk is of increased or more sophisticated phishing attacks to obtain further details such as passwords.

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 experienced in 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, Let your dependents know what has happened and that they should be alert to any emails, phone calls or text messages from unknown sources.

5, Additional support.

Attached to this message is information on Experian's identity theft monitoring service, which Halma is offering to all those affected by the data breach – this includes former employees and their dependents who have had their data accessed. The service provides added protection through:

- Monthly privacy scans to find and help remove your personal info from sites
- Identity theft monitoring, alerts and dark web surveillance
- Fraud resolution and up to $1 million ID theft insurance, subject to the policy conditions
- Easy locking and unlocking of credit files with Experian CreditLock

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 [contact].

You will find an FAQ attached to this message and, if you are still accessing UKG, the information is also there. If you can't find the answer to your question then please let me know.

[Name]

[Title]