15566

MESSAGE FROM EUAN MUNRO

TUESDAY 16 JULY

To all Aviva Investors Employees:

I regret to inform you that we detected a data breach within Aviva Investors yesterday. We are taking this matter very seriously and during the course of today have carried out prompt and thorough investigations to assess the situation in more detail. We understand the importance of communicating with you in a situation like this so that you can take all necessary precautions and be especially vigilant.

The facts are:

- This employee and contractor data was sent to an external email address by a contractor, shortly before their contract ended and was detected by our data security software.
- The information includes personal details of Aviva Investors' staff and contractors globally – name, date of birth, salary information, passport number and national/tax identifiers e.g. UK National Insurance numbers.
- No bank details are contained within the breach. Whilst at this stage we have no reason to believe that the ex-contractor had criminal motives, we cannot entirely discount the possibility that the data could be used for malicious reasons, potentially including identify fraud.

We are so sorry that this has happened and will do everything we can to support and look after our people. Aviva will ensure that employees will not suffer any financial loss as a result of this incident. This incident is limited to Aviva Investors employees only and does not affect any clients, Aviva customers or other Aviva employees. We are taking all necessary actions as urgently as possible and the appropriate authorities have been notified. We are continuing our investigations and will update you as soon as we have further information.

In the meantime, measures you can take to protect yourself include:

- please be vigilant and monitor your online accounts for unexpected activity
- avoid and delete anything that may be a phishing email (see below for some guidance on how to spot suspicious emails)
- report any suspicious activity to askciso@aviva.com

You may have concerns. I've made myself available all day tomorrow so if you have any questions, please drop me an email.

Euan Munro
Chief Executive Officer, Aviva Investors

Additional notes:
A phishing email will typically contain a malicious attachment or a link to a malicious website. As well as awareness, the best defence is to make sure that your devices and software are kept up to date. We recommend the following guidance: https://www.cyberaware.gov.uk/.

While phishing emails are designed to be difficult to spot, there are some checks which you can employ in order to identify the less sophisticated campaigns:

- **Sender.** Were you expecting this email? Not recognising the sender isn't necessarily cause for concern but look carefully at the sender's name – does it sound legitimate, or is it trying to mimic something you are familiar with?
- **Subject line.** Often alarmist, hoping to scare the reader into an action without much thought. May use excessive punctuation.
- **Logo.** The logo may be of a low quality if the attacker has simply cut and pasted from a website. Is it even a genuine company?
- **Dear You.** Be wary of emails that refer to you by generic names, or in a way you find unusual, such as the first part of your email address. Don't forget though, your actual name may be inferred by your email address.
- **The body.** Look out for bad grammar or spelling errors but bear in mind modern phishing looks a lot better than it used to. Many phishing campaigns originate from non-English speaking countries but are written in English in order to target a wider global audience, so word choice may be odd or sound disjointed.
- **The hyperlink/attachment.** The whole email is designed to impress on you the importance of clicking this link or attachment right now. Even if the link looks genuine, hover the mouse over it to reveal the true link. It may provide a clue that this is not a genuine email. If you are still unsure, do not click the link – just open a webpage and log onto your account via the normal method. If it appears to be from a trusted source, consider phoning the company's customer service, but never follow the email's instructions. Be aware that some companies operate policies stating they will never include links in emails and will never ask for personal information. Again, if in doubt, open a browser and check – and do not open attachments.
- **Signature block.** The signature block may be a generic design or a copy from the real company.

MESSAGE FROM EUAN MUNRO

WEDNESDAY 17 JULY

Company confidential

To all Aviva Investors Employees:

Following my note to you yesterday, here is an update on the data loss within Aviva Investors, with further clarity following our investigations and in response to questions we've received from you today.

Our investigations confirm that:

- personal email addresses were included in some instances
- home addresses were not included.

We've have been asked what we mean by national/tax identifiers, so for clarity:

- if you are in the UK this could be your National Insurance number
- if you are in the United States it would be your Social Security or the equivalent depending on the country you're in.

Our further analysis has confirmed that contractors' personal details were not included.

I'd like to emphasise that no bank details were contained within the data.

We have made contact with the individual concerned and they are co-operating with our investigation.

Keeping you safe

Our Cyber Threat and Intelligence team are scanning the web for suspicious activity and nothing has been found thus far.

We will provide you with identity theft protection such as Experian or equivalent expert providers in your region. This service will give you access to a system and tools to help mitigate identity theft risk. We will provide further details as soon as they are available.

We've also setup a dedicated mailbox and team to deal with any of your queries regarding this incident. If you have any concerns or questions, please send these to dataquestions@avivainvestors.com.

We encourage you to please be vigilant and monitor your online accounts for unexpected activity. Please remember that Aviva monitor all emails sent out externally.

I would like to reiterate that:

- Aviva will ensure that no employee will suffer any financial loss as a result of this incident.
- this incident does not affect any clients, Aviva customers or other Aviva employees.

My leadership team and I will continue to do everything we can to support and look after our people and will update you as soon as we have further information.

Euan Munro
Chief Executive Officer, Aviva Investors

15566

[redacted]

From: [redacted]
Sent: Wednesday, July 17, 2019 5:05 PM
To: [redacted]
Subject: Data Breach: What You Can Do

Aviva Investors: Confidential

Company confidential

As a follow-up to Euan's email regarding the breach in employee information, we are sending the below to our U.S. employees to assist with possible security measure you can take. We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus or complete the online form by clicking any one of the links below. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.
Equifax: equifax.com or 1-800-685-1111
Experian: experian.com or 1-888-397-3742
TransUnion: transunion.com or 1-888-909-8872

Request that all three credit reports be sent to you, free of charge, for your review. 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. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

We are so sorry that this has happened and will do everything we can to support and look after our people. You will be provided identity theft protection such as Experian or equivalent expert providers. This service will give you access to a system and tools to help mitigate identity theft risk. We will provide further details as soon as they are available. We've also setup a dedicated mailbox and team to deal with any of your queries regarding this incident. If you have any concerns or questions, please send these to dataquestions@avivainvestors.com. We encourage you to please be vigilant and monitor your online accounts for unexpected activity. We will provide future communications about additional measures AI is doing to help employees navigate this situation.

Regards,

Jamie Shields, IACCP
Chief Compliance Officer | Aviva Investors Americas LLC
+1 312 873 5848 | M: +1 312 350 7221
E: jamie.shields@avivainvestors.com
Aviva Investors, 225 W Wacker Drive, Suite 2250. Chicago, Illinois, 60606
www.avivainvestors.com

MESSAGE FROM EUAN MUNRO

FRIDAY 19 JULY

Company confidential

DATA LEAK - IMPACTS ON YOU

Dear [redacted],

Following my earlier communications about the data leak this week, we have continued to investigate the situation. Unfortunately, we have discovered that your personal email address details were included.

We would like to apologise for any inconvenience caused. Please be extra vigilant and monitor your online accounts for unexpected activity. You can follow the below steps to help protect yourself:

1. If you have anti-virus software installed on your computer, run a full system scan to make sure it isn't infected.
2. If you suspect any suspicious activity, reset your password for any logins that use your personal email address – choose a strong, separate and memorable password and never use a password more than once between different accounts.
3. Be vigilant when opening emails particularly if you weren't expecting it and it comes from somebody you don't recognise.
4. Do not click on links or open attachments in suspicious emails - delete any emails you feel are suspicious.
5. Keep all your devices and apps up to date by installing any updates provided by the manufacturer.
6. Review your recent sent/deleted and received emails for any suspicious activity – if you detect any, notify your email service provider
7. Visit the Cyber Academy for additional information and support.

At this stage we still believe that there are no criminal motives, but we cannot entirely discount the possibility that the data could be used for malicious reasons. Please be assured that our Cyber Threat and Intelligence Team are continuing to monitor the situation closely and thus far nothing has been found.

My leadership team and I will continue to do everything we can to support and look after our people and will update you as soon as we have further information. If you have any concerns or questions, please send these to dataquestions@avivainvestors.com.

Euan Munro
Chief Executive Officer, Aviva Investors

MESSAGE FROM EUAN MUNRO

MONDAY 5 AUGUST

To all Aviva Investors Employees:

Following my recent communications, I wanted to update you on the data leak from within Aviva Investors which affected Aviva Investors employees.

We have now completed our investigations and can confirm that although the data was sent to a personal email address, we have found no evidence to suggest it was forwarded on any further.

Following a review, the Data Loss Protection Tool has been reconfigured and you can expect to see further protections and restrictions on data handling and sharing in the coming months.

This does not mean there is no risk, which is why we still encourage you to continue to be vigilant and monitor your online accounts for unexpected activity. Please report any suspicious activity to askciso@aviva.com.

In response to your queries we have emailed all employees whose personal email addresses were included in the data. We have provided identity theft protection such as Experian in the UK or equivalent expert providers to all regions where such products are available.

Our Cyber Threat and Intelligence team will continue to scan the web for suspicious activity. If you have any further queries regarding this incident, or any concerns or questions, please send these to dataquestions@avivainvestors.com.

As I said previously, I am very sorry this has happened, I appreciate it caused a lot of concern, but I would like to reiterate that:

- Aviva will ensure that no employee will suffer any financial loss as a result of this incident.
- This incident does not affect any external Aviva Investors clients, Aviva customers or other Aviva employees.

My leadership team and I will continue to do everything we can to support and look after you and will update you if there is further information, however, we expect this to be our last communication on this topic.

Euan Munro
Chief Executive Officer, Aviva Investors

APPENDIX B

CERTIFICATION OF CREDIT MONITORING SERVICES

On behalf of Aviva Investors Americas LLC, I hereby certify that credit monitoring services were provided to consumers in compliance with G.L. c. 93H, § 3A.

Jamie Shields
Chief Compliance Officer
T: (312) 873-5848
E: jamie.shields@avivainvestors.com
Aviva Investor Americas LLC