BROOKE
ACTION FOR WORKING HORSES AND DONKEYS

Cyber attack on MoveIt by Clop – Updated Wednesday 21 June 2023

What is it?

You may have seen increased news coverage in the past three weeks of a global cyberattack by a Russian cyber-criminal gang called Clop. It appears that their intention is to demand a ransom from various institutions including European manufacturers, US-based investment firms and US universities. This issue has affected many UK organisations such as BBC, British Airways, Boots, Aer Lingus and even the UK's broadcasting regulator, Ofcom.

Has Brooke been affected?

Yes. On Friday 9 June 2023, Brooke was informed that one of our historic suppliers (DDC Outsourcing Solutions – referred to as DDCOS from hereon) was affected by a technological vulnerability in a system called MoveIt. They used this tool for the movement and storage of files. A recently identified vulnerability of this tool enabled the Clop hackers to gain access to the system and to potentially see content stored in the tool for a period of 2.5 hours.

Has my data been affected?

Cheques made payable to Brooke from December 2020 to October 2021 were affected. The data stored in the tool by DDCOS was back-up copies of cheques as a business continuity

measure to ensure donations could be made in result of any technical failures.

What data could have been accessed?

The scanned image of the cheque contains the following information:

- Name of your bank
- Name of the cheque issuing branch
- Who you have made the cheque payable to (in this case, Brooke)
- The amount
- The date
- Your name as it appears on your bank account
- Your signature
- The Cheque Number
- Bank Sort code
- Bank Account Number

Could my data be used fraudulently?

None of the bank information on the cheques could be used to compromise bank accounts.

Cheques cannot be used as a valid form of identification and could not be used to set up new accounts for services or products.

The back-up copies of cheques could not be amended and re-presented as the cheques have already been claimed and so we believe the risk to Brooke Supporters is minimal.

There is a minimal risk of cheque fraud if a cheque were to be counterfeited but we believe this risk to be small and would advise keeping an eye on all bank statements.

What can I do if I am affected?

Again, we believe the risk to supporters to be very minimal in terms of fraud or identity theft but if you are concerned, we would recommend that you check your bank statements and ensure that the payments showing are those you have made and contact your bank immediately if you do not recognise anything on your statement.

You can:

- Visit Action Fraud – to report incidences of fraud and cybercrime.

- Visit Fraud Prevention | Identity Fraud | Protective Registration | Cifas – to find out more or request to be added to the National Fraud Database which alerts companies using CIFAS to pay special attention when details are being used to apply for products and services.

- Consider registering with the three credit reference agencies and logging a fraud alert. Once you have placed a fraud alert on your credit report with one bureau, they will alert the others. The three companies are:
    - Credit Scores, Reports & History | Equifax UK
    - Experian | Credit Scores, Reports & Credit Comparison

- TransUnion UK | TransUnion UK

- Visit Identity theft | ICO – to learn more about identify theft and what to do.

- Contact your bank.

Has the Regulator been informed?
Yes. As soon as the breach was reported to Brooke, we took action by investigating the issue and submitting a report to Information Commissioners Office (ICO). We worked with DDCOS to ensure all data was removed and secured should further investigations be required by the ICO. All data will be securely deleted once investigations are complete and the case is closed.

DDCOS also reported the issue directly to the ICO.

Will DDCOS be held to account for the potential data breach?
As this has been reported to the ICO, they will investigate and take action as required. The ICO will issue recommendations if fixes are required and will serve penalties and fines as they deem relevant. The ICO publish their enforcement actions online at Enforcement action | ICO.

Do you still work with the organisation who were hacked?
No we do not. We ended our contract with this organisation in October 2021 and were informed that Brooke's data had been deleted. Unfortunately they had failed to check the MoveIt tool DDCOS used.

We work with an organisation called Mosaic Fulfilment Services and have been doing so since October 2021. They have confirmed that they do not use the MoveIt tool that was compromised and have never done so during the period of our contract with them.

Who else has been affected?

For more information in the news about this issue please visit:

Hacker gang Clop publishes victim names on dark web - BBC News

BA, Boots and BBC staff details targeted in Russia-linked cyber-attack | Cybercrime | The Guardian

BA, BBC and Boots staff data hit by Russia-linked cyber attack (telegraph.co.uk)

Thousands of workers affected by major data hack at BBC, BA and Boots linked to Russia - Mirror Online

Which companies were affected by the MOVEit Russian payroll hack? | Evening Standard

What will happen next?

Clop, the cyber-criminal gang responsible for this global hack, is expected to engage with organisations to extort ransom

payments by threatening that data they have accessed will be shared more widely. At this point in time, neither Brooke nor DDCOS have been approached with a ransom request. We also do not believe that the data that could have been accessed is sensitive enough to warrant a cause for concern.

The ICO will inform Brooke and DDCO if further steps need to be taken and we will update this page with that information.

If you need further information on any of the above please contract our Supporter Care Team on 020 7470 9393 or email info@thebrooke.org.