Ministry of Defence

MINISTRY OF DEFENCE
FLOOR 5, ZONE D, MAIN
BUILDING, WHITEHALL
LONDON SW1A 2HB

7 May 2024

Dear Member of the Armed Forces,

We are writing to inform you of a compromise to an Armed Forces payment network. This is an external network, separate to MOD's core systems, and is not connected to the main military HR system - JPA. This is operated by a contractor. All functions within the JPA system have continued securely throughout.

This incident potentially impacts personal data of current regular and reservist personnel and a small number of veterans. The data includes names and bank details, and for a small proportion of individuals, addresses.

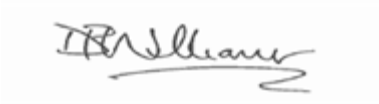
We want to reassure you that we have taken immediate remedial action, taking the network offline to minimise risk. Our initial investigations have found no evidence that any data has been removed from the network, but we will continue to investigate, working closely with other agencies. We have also launched a full review, drawing on specialist external and Cabinet Office support and expertise. We are also investigating potential failings by the contractor.

Specialist advice, guidance, and support is available on gov.uk, and Defence websites. We have also purchased independent licences from a commercial data protection service. This can be accessed through a personal device of your choice, providing you with constant monitoring of your personal data - notifying you of any irregular activity. Registration codes and a how-to-guide will be provided shortly. As always, and where necessary, there is access to welfare and financial support. Please use your chain of command if required.

Everyone was paid as normal in April, and we are confident that salaries for May will not be affected. You may have however noticed a slight delay in the payments of routine expenses. We are in the process of restoring normal systems, and a solution is in place to ensure we facilitate all outstanding expenses payments which should be paid by the end of the week. High value payments continue and all outstanding Forces Help To Buy and Terminal Benefits payments have been paid by a BACS transfer. If you have not received expected payments, please get in touch with your HR teams as a priority.

If you see your details online or published somewhere, you must report it immediately to Defence Business Services via the helpline. Do not attempt to edit or delete the data, do not contact the website owner and do not engage with anyone who claims to have identified you.

Whilst this will undoubtedly result in increased levels of anxiety - for which we apologise - the support and guidance we have provided will help keep your data protected and you safe. We will do all we can to keep you updated.



DAVID WILLIAMS

PERMANENT SECRETARY

GENERAL GWYN JENKINS

VICE CHIEF OF DEFENCE STAFF

07 May 24

Network Compromise Frequently Asked Questions

1. Why did we find out from the media about this incident before we were told internally?

Defence was made aware through Service providers of a potential network compromise and was in the process of informing you following the bank holiday weekend. It is unfortunate that our intent to proactively communicate to you, detailing the action we have taken, was overtaken by media activity.

2. What is the nature of the compromise?

The Ministry of Defence is aware of and investigating a compromise of an independent network system. The system is not linked directly to JPA. The system transmits pay related data over the internet. Pay related data potentially includes personal data of members of the Armed Forces.

3. What specific personal data may have been compromised?

Whilst there is no evidence to suggest that any data has been compromised, the system transferred payroll information to your bank enabling payment. Data included your name, Service Number, and bank details. Whilst forensic investigations are ongoing, it is also apparent that a limited number of addresses were retained within the system. No other personal data from JPA is held in this system.

4. How will I know if my Home address has been potentially compromised?

Whilst we continue to investigate the nature of the breach, there may be a small number of personnel whose address is include as data on the system. Address data may be your place of work, your administration address, or Home Address. Those whose home address is identified are in the process of being written to.

5. Was the JPA system compromised?

No, the compromise is associated with an independent stand-alone system which only transmits pay related instruction over the internet.

6. Whose details are involved in the compromise?

The system concerned is used to transmit details to banks facilitating payments for Regular, Reserve, and Cadet Adult Volunteer force personnel. Whilst investigations continue, it is possible that some legacy data detailing the payment to those who left the Service, but have received a payment from 2018 may also be included. Forensic investigations are ongoing to refine who may have been affected.
MyHR is not affected by this incident. Payment details of Civil Servants and members of the Royal Fleet Auxiliary are not affected.

7. I am a Veteran. Am I affected by this?

We have written to all those veterans who have left from Jan 2018 onwards, and in receipt of a payment from the MODs payment system. It is possible that these veterans may be affected by this potential compromise.

8. What has the MOD done about this?

Defence takes its responsibility for your data very seriously. Once we were aware of the incident, we stopped the processing of all payments, isolating the systems to enable us to review what may have happened. Whilst conducting this investigation and to minimise the impact to our people, we put in place alternative payment methods for high priority payments (Forces Help to Buy / Early Departure Payments). Owing to the large number of lower value payments, e.g. travel and subsistence, you may have experienced a delay with these claims last week. The team has worked hard to provide assurances that new systems are safe, and we expect to recommence a full payment service later this week. We are sorry that for a small number of personnel this may mean a delay of a few days in payment of some of these claims.

Whilst we do not currently have any proof that any of your data has been compromised, we must be prudent and assume that it may have been. To provide you additional protection, we have purchased licences with a market leading personal data protection service which you will be able to access on a device of your choosing. This will assist in the assurance, safety and security of your data. A guide to obtaining your activation code will be sent out today. The system will provide you with early warning and alerts detailing any unauthorised use, or exploitation of your personnel data on either the internet or dark web.

We realise however that for some, this news may cause some anxiety. As always you are encouraged to highlight any welfare or financial concerns to your chain of command. For those who are not able to use local support networks, a dedicated phone line has been established. This number is 01249 596665 or e-mail DBS-Informationline@mod.gov.uk

9. Is my personal data in the public domain?

There is no evidence that because of this incident, your personal data is in the public domain. Your continued vigilance, further enabled by the protection service will provide the assurance you deserve. Should we become aware of any change in this guidance, we will immediately inform you through your chain of command or subsequent correspondence.

10. Is my personal data likely to be exploited?

We have no indication that any data has been compromised or exploited. We will offer further guidance to address any irregularities - if they are detected. The data protection service in which we are investing will continue to monitor for web-based activity irregularities, immediately alerting you, and detailing advice on what action to take.

11. Can you reassure me that this data is not going to be publicly released.

There is no evidence suggesting that any data is publicly available. This is being actively monitored. The UK's various cyber defence entities actively search for threats and monitors every part of the Internet. If the data associated with Armed Forces personnel is released into the public domain, Defence Digital will be notified. This is in addition to the personal notification that will be sent to you via the data protection service.

12. Has the Information Commissioner's Office (ICO) been made aware?

Yes.

13. Has an investigation been launched?

The Secretary of State for Defence has directed an independent investigation by an external organisation which commenced on 6 May. This will determine causes and enable lessons to be identified.

14. What can I do to safeguard myself from identity fraud?

There is no requirement for you to do anything immediately, but you could consider a review of cyber best practice; for example, reviewing your personal social media privacy settings. You may also consider opting out of the open electoral register (link below).

www.ico.org.uk/for-the-public/electoral-register

If you become aware of any unexpected activity, it may be sensible to change associated passwords or speak to your bank.

You will be provided an activation code for a world-leading data security protection service, providing you and your family with the assurance you deserve. For those serving, details explaining how you can obtain your activation code will be promulgated today. For those serving independently, or if your loved one is deployed, specific arrangements have been put in place by the chain of Command. If in doubt, please contact local support network.

We are in the process of generating an automated system for small proportion of veterans and Cadet Adult Volunteers affected by the issue. If this applies to you, you are advised to dial the call centre 01249 596665 or e-mail DBS-Informationline@mod.gov.uk

15. If I enrol in the personal data protection service, will that impact my credit score?

These services do not interact with the credit scoring system or report to the credit bureaus. There is no direct impact on your credit score from activating this service.

16. Are there any types of activity I might expect to see on my accounts that might indicate it is compromised?

At present we have no indication that this data has been exploited, but it is prudent to remain vigilant and continue to review your statements for unauthorised payments.

Whilst you are probably already doing this, the following six signs are worth looking out for:

- Watch for any unauthorised activity: Always know what transactions are expected. Even the smallest unauthorised transfer can be a warning sign.

- Don't ignore notifications: If you get an email saying your account details have changed and you didn't change them, your account may be compromised.

- Beware of bogus calls: If someone phones and claims to be from your payment provider, insist on calling them back on the company's public phone number.

- Don’t trust the text: If you suddenly start getting messages or calls from a mobile number that your provider doesn’t normally use - be very suspicious.

- Check every email: If an email or other online communication doesn’t look genuine, don’t reply to it without checking with your provider.

- Look out for bogus links: If you see strange activity on your account, check to see if you’ve recently clicked on any retrospectively suspicious links.

Banks routinely monitor your account and report unusual activity. Most banks also use two factor authentication. You are encouraged to use these techniques if available. It is likely that your bank will be in touch with you if they detect anything suspicious with your account.

17. What does this mean to my military payments?

- **Next main payment in May**. Owing to our intent to recommence T&S payments this week we are confident that this issue will be fully resolved before the next pay run in May.

- **What will happen to my expense’s claims?** Claims inputted in JPA after 29 Apr 24 may have been subjected to a slight delay. We are confident a full solution will be in place this week facilitating the payment of outstanding claims. If this is causing you an issue you should contact your local HR team. If you are experiencing broader financial issues, please get in touch with your pay specialists as a priority.

- **My Forces Help to Buy payment.** All outstanding payments have been facilitated by BACS transfer. If you have any queries, please get in touch with your pay specialists, or contact the JPAC Enquiry Centre on 0141 224 3600.

- **Terminal Benefits Payment.** All outstanding payments have been facilitated by BACS transfer. If you have any queries, please get in touch with your pay specialists, or contact the JPAC Enquiry Centre on 0141 224 3600.

We are determined that you will not be financially disadvantaged owing to this issue. Should you incur any such costs, or believe you have been, please contact your local pay specialist as a priority.

18. I split my pay between other accounts, and other people. Could their data have also been compromised?

We have no indication that any data has been exploited. If you transfer an element of your pay to another account at source (i.e. directly from JPA), it would be prudent to advise them that there is a possibility that this may have occurred. The commercial data protection service we are providing will also be made available to them if required. You should highlight this requirement to your line management in support of obtaining a second licence.

19. Are my pension payments affected?

No. Pensions are paid via a separate system and are unaffected.

20. Is my War Pension Scheme payments or my Armed Forces Compensation Scheme payment affected?

No. These payments are paid via a separate system and are unaffected.

21. Can I claim any costs incurred as a direct result of being paid later than I expected?

If you incur additional cost as a result of late payment of expenses, you are to contact your chain of command/Unit HR with proof of additional costs. Claims will be dealt with on a case-by-case basis.

22. What broader support is available to me?

If you experience / notice any suspicious activity, you should contact your chain of command immediately. All personnel are advised to look out for official sounding emails about resetting passwords, and to be wary of messages requesting confirmation of identity or being urged to take immediate action. The MOD's guide - Advice and Guidance-Compromise of personal information Protecting Your Privacy and the National Cyber Security Centre's Data breach guidance for individuals - NCSC.GOV.UK are good starting points for information. They document the immediate actions you must undertake to safeguard your personal information and detail other additional preventative measures you may wish to take.

The National Counter Terrorism Security Office (NaCTSO) has also produced a useful and comprehensive Guide to Personal Security. Recommendations contained within this guidance are primarily common-sense precautions, albeit not exhaustive. Their usefulness will depend on your personal circumstances, but are based on research, lessons learned from historic events, expert advice and best practice.

The following resources may also be helpful:

- How to tighten the security on your social media accounts and Other tips for staying secure online
- The electoral register and the 'open register': Opt out of the 'open register' - GOV.UK (www.gov.uk)
- www.ico.org.uk/for-the-public/electoral-register
- Remove your details from UKPhoneBook (Orbis)
- Remove your details from 192.com

The Think Before You Link app can be downloaded to your personal devices. The app provides tutorials on the importance of and how to manage your digital footprint as well as guidance on how to recognise a potentially malicious approach online.

We have also obtained an operating licence for to a world class data security protection service. Further details will be promulgated today. For the non-serving community, an update will be provided on 01249 596665 or via an e-mail sent to DBS-Informationline@mod.gov.uk

For those in the Armed Forces, the TLB Principal Security Advisor teams remain available to provide advice should it be required. Contact details are available at the Def net sy and Resilience Portal on SharePoint.

23. Should I change my personal banking details?

This is of course a personal decision, but as stated above we have no evidence implying the compromise of any personal data. We are providing you with a commercially available data protection service purely as a prudent and sensible precaution. The service will monitor your data and if any activity of concern is detected, you will be alerted with guidance on what to do next.

24. **What should I do if my personal details are published and who can I contact if I have any security related questions?**

You should submit a Security Incident Report Form (SIRF) and inform your Chain of Command. When a SIRF is submitted on the internet, it is reviewed by MOD security personnel and subjected to an initial security risk assessment, with further action taken on a proportionate basis. If you discover your details online you must not attempt to edit/delete the data and/or attempt to contact the website owner. Instead, provide the details on the SIRF so it can be assessed by security personnel. Separately, if you are directly contacted by anyone who claims to have identified you, do not engage. Report the encounter via a SIRF providing the details so it can be assessed by security personnel.

If you have any further security related questions please contact your Warning Advice & Reporting Point (WARP). If not on MODNET contact the Joint Security Coordination Centre on 07768 558863. Personnel can also contact coo-dsr-jsyccoperations@mod.gov.uk.