ico.
Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

[redacted]

By email only to: [redacted]

21 April 2021

Dear [redacted]

Case Reference Number: INV/0023/2021

I am writing further to our acknowledgement of the personal data breach you notified us of on 14 December 2020.

Specifically, HM Revenue and Customs (HMRC) discovered on 2 December 2020 that a breach had occurred on 19 June 2020. An organised crime gang (OCG) used 160 National Insurance Numbers (NINOs) to set up bogus Government Gateways. [redacted]

Based upon the information provided to us so far, we have decided that this case requires further investigation.

I am the case officer in charge of that investigation.

I am investigating HMRC's compliance with data protection legislation, i.e. the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

In particular, we are investigating your organisation's compliance under Article 5(1)(f) of the GDPR. As you may be aware, this requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

At this stage we are still investigating the circumstances reported to us and we have not yet formed a view on what action, if any, we will take. However, it is possible that, once we have considered all the relevant evidence, we will exercise our powers as set out in the attached leaflet.

Article 31 of the GDPR sets out a general obligation on controllers and processors to cooperate, on request, with the supervisory authority in the performance of its tasks. Your cooperation in providing full and detailed answers to our enquiries and establishing the facts is therefore required. Such cooperation will be taken into account in relation to the outcome of our investigations.

Further information

In order that I may assess this matter and determine what, if any, further action may be necessary, please provide the following information:

Breach

1. Please provide a copy of your internal investigation report in connection with this incident. In the event there is no investigation report, then please provide as much detail as possible as to what happened and how this incident occurred.

2. If not explained in your answer to the previous question, please provide responses to the following:

    i. Please confirm the number of data subjects and records affected by the breach.

    ii. Please confirm if the OCG created new customer accounts, or did it access existing genuine customer accounts, or both. Please provide a breakdown of the numbers involved.

    iii. It is understood the OCG used hijacked NINOs to set up bogus Government Gateway accounts [redacted] Other than a NINO, was any other personal data used by the OCG to set up the bogus accounts? Please provide full details.

    iv. Are HMRC able to confirm if the personal data used by the OCG to access (or create) customer accounts was from an external source (to HMRC)? Or did the personal data in this respect originate from HMRC? Please provide any available information in respect of this aspect.

    v. In what way did the OCG use [redacted]

vi. Please explain in as much detail as possible how once the OCG had set up the bogus accounts, that it was then then able to access Personal Tax accounts (PTAs) of genuine customers.

vii. It is understood that the OCG [redacted] please provide full detailed breakdown of the personal data which was obtained by the OCG, including the number of records and data subjects affected by this aspect of the breach.

viii. It is understood that there are indications that in some instances the actions of the OCG diverted payments that would have gone to genuine customers. Please confirm if these losses were suffered by HMRC, as opposed to the data subjects. If data subjects suffered financial losses, please provide further details as to the losses suffered and the actions taken by HMRC to mitigate this.

3. It is noted that there has apparently been access to DWP data. Please provide responses to the following:

   i. How and in what way was the OCG able to access DWP data.

   ii. What DWP data did the OCG have access to; please provide full details, including the number of data subjects and records affected and the type of data compromised.

4. Did your organisation's identification verification processes contain adequate fraud prevention measures to prevent fraudulent access to a customer account, or the new registration of a fraudulent customer or account? Please provide any relevant details regarding the measures in place at the time of the breach.

5. Were there any other measures in place to prevent fraudsters creating new accounts with stolen/hijacked identities, or accessing existing genuine customer accounts?

6. Is your organisation liaising with law enforcement agencies regarding this breach? If yes, please advise which agencies and advise the extent of their involvement.

Data subjects

7. It is understood from the breach report that your organisation has not informed the data subjects about the breach, as the incident did not meet

the threshold for communicating it to the data subjects. In relation to this, please provide answers to the following:

i. Please detail why you felt such notification would not be necessary in this instance.

ii. Please provide an update; has this position changed? If so, please advise how it has changed, and (if applicable) how and when the data subjects have been informed of the breach.

8. Has an analysis taken place of all the data subjects' records affected by the breach? If so, please provide full details and in particular advise whether any personal data was altered or deleted by the fraudsters, alongside any other information you feel is relevant. If an analysis has not been carried out, then please explain the rationale for not undertaking this work.

9. If not answered in response to the previous question, have any data subjects' records or accounts been rendered inaccurate by the breach? If yes, please provide full details, including how many data subjects' records have been affected and what action HMRC are taken in this respect to correct these records.

10. It is noted from your breach report that it was "not yet known" if this breach resulted in a high risk to the data subjects. Please confirm what the current position is. If you have subsequently assessed that the data subjects are at high risk, please provide full details, including any potential or actual harm to the data subjects.

11. Has your organisation received any complaints from any data subjects affected by the breach? If yes, please provide details and sample extracts (redacted of personal data) from the complaints detailing the harm the data subjects have suffered where applicable.

Mitigating action

12. Have the data subjects' accounts or records which have been affected by this breach been secured to prevent the fraudster accessing them again? If so, please confirm the date(s) or date range in which they were secured.

13. Has your organisation taken any other mitigating action to lessen the effects of this breach? If so, please provide any relevant details.

Remedial steps

14. It is noted that [redacted] In relation to this statement, please provide responses to the following:

    i. [redacted]

    ii. [redacted]

    iii. [redacted]

    iv. [redacted]

15. [redacted] Has your organisation identified any risk to customers' personal data being compromised before this type of breach is discovered? If yes, please provide details, including any relevant risk assessment undertaken.

16. It is stated that your organisation is [redacted] If not explained in answers to previous questions, please provide responses to the following:

    i. [redacted]

    ii. [redacted]

    iii. [redacted]

17. Please advise of any remedial steps your organisation has taken to prevent a recurrence of such an incident.

Policy and Procedure

18. Do you consider this incident to have breached any of your organisations policies or procedures? If so, please confirm which policies or procedures, and provide either copies or relevant extracts. Please also advise how these policies or procedures were brought to the employee's attention.

If you have any further information relevant to this matter, including any additional remedial measures taken or changes to your policies, procedures or technical security, please provide full details when responding.

Please ensure any correspondence is sent to [redacted]

Please provide the information requested **by 05 May 2021.** If this deadline is not reasonable in the current circumstances (COVID-19), please do let us know and we will work with you to agree a reasonable deadline.

Please contact me if you wish to discuss this case.

Thank you for your assistance in this matter.

Yours sincerely

Polly Greenwood
Lead Case Officer
Investigations
Information Commissioner's Office
0330 313 1699

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

The ICO publishes the outcomes of its investigations. Examples of published data sets can be found at this link (https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/).

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice

The Information Commissioner's powers

Data protection incidents which occurred prior to 25 May 2018 fall under the Data Protection Act 1998 (the DPA 1998) which was in place until that date.

Incidents which occurred on or after 25 May fall under the General Data Protection Regulation (the GDPR) and/or the Data Protection Act 2018 (the DPA 2018), which we refer to as the 'data protection legislation', depending on the nature of the processing involved.

There are a number of powers available to the Information Commissioner's Office (ICO) in respect of breaches of the data protection legislation.

Our powers are not mutually exclusive. We will use them in combination where justified by the circumstances.

The main options are to:

- provide practical **advice** to organisations on how they should handle data protection matters;
- conduct **consensual assessments** (audits) to assess whether an organisation's processing of personal data follows good practice;
- issue **information notices** requiring individuals, controllers or processors to provide information as part of an investigation into compliance with the data protection legislation. If the recipient of an information notice does not provide a full and timely response, the ICO may apply for a court order requiring compliance with the information notice;
- issue **assessment notices** to allow us to investigate whether a controller or processor is compliant with data protection legislation. The notice may, for example, require the controller or processor to give us access to premises and specified documentation and equipment;
- issue **warnings** where proposed action threatens non-compliance with data protection legislation;
- issue **reprimands** for infringements of relevant data protection legislation;
- issue **enforcement notices** where there has been an infringement, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the data protection legislation;

- issue **penalty notices** requiring organisations to pay administrative fines of up to 20 million Euros, or in the case of an undertaking, up to 4% of the total worldwide annual turnover, depending on the nature of the infringement; and

- **prosecute** those who commit criminal offences under the data protection legislation. In Scotland, where the ICO is satisfied that there are grounds for a prosecution, it will make a report to the Procurator Fiscal to make a determination whether or not to prosecute.

The ICO are also the Competent Authority for Relevant Digital Service Providers (r-DSPs) under the Network and Information System Regulations (NIS regulations).

The NIS regulations came into force on 10 May 2018 and aim to establish a common level of security for network and information systems. These systems play a vital role in the economy and wider society, and NIS aims to address the threats posed to them from a range of areas, most notably cyber-attacks.

There are a number of powers available to the ICO in respect of breaches of the NIS regulations.

- **Information Notices:** requiring an r-DSP to provide information to enable the ICO to assess the security of it's systems and the implementation of its security policies;
- **Powers of Inspection:** to assess if an r-DSP has fulfilled its requirements in identifying and taking appropriate and proportionate measures to manage the risks posed to organisations who provide an online marketplace, online search engine, or cloud computing service;
- **Enforcement Notices:** may be served if;
    - the r-DSP has failed in taking appropriate and proportionate measure to manage risk;
    - Failed to report a NIS incident;
    - Failed to comply with the notification requirements of NIS;
    - Failed to comply with an Information Notice;
    - Failed to comply with a direction given by the Commissioner.
- A **Penalty Notice** may only be served after the issue of an Enforcement Notice under NIS when;
    - The r-DSP was instructed to take steps to rectify a failure and failed to do so;
    - Or the Commissioner is not satisfied by the representations made by the r-DSP in regards to their response to an Enforcement Notice;
    - There are three tiers of penalty notice ranging from £1million to £17 million.

The Commissioner is also responsible for ensuring organisations comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended. These regulations establish rules by which organisations that engage in electronic marketing to individuals must comply.

To ensure this the Commissioner has the power to

- Provide practical advice and guidance;
- To issue third party information notices in order to identify organisations that are sending unsolicited marketing communications;
- Issue information notices compelling organisations to answer questions regarding their processes;
- Issue both enforcement notices to ensure future compliance and monetary penalties up to a maximum of £500,000 in response to previous non-compliance with the Regulations.

The Regulations also place an onus on communications service providers to notify the Commissioner of any security breach with 24 hours of the breach being detected. Failure to comply with the reporting timescales can result in a fixed fine of £1000 being issued.

Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

[redacted]

10 December 2021

[redacted]

Case reference number: INV/0023/2021

I write to inform you that the ICO has now completed its investigation into the personal data breach you notified us of on 14 December 2020.

On 02 December 2020 HM Revenue and Customs (HMRC) discovered that a breach had occurred on 19 June 2020. An organised crime gang (OCG) had used 193 genuine National Insurance Numbers (NINOs) to set up bogus Government Gateway (GG) accounts. [redacted] This enabled the OCG to carry out enrolments on the bogus GG accounts of genuine Self-Assessment (SA) customer Unique Tax References (UTRs).

What ultimately followed was the submission of fraudulent 2019/20 returns on SA accounts, with the aim of the OCG being to make fraudulent expenses claims.

Also, it was discovered that details belonging to 130 of the data subjects were used during the duration of the breach to utilise the Department of Work and Pension's (DWP) Universal Credit (UC) service.

This case has been considered under the General Data Protection Regulation (the GDPR) due to the nature of the processing involved.

Based on the information you have provided; we have decided that regulatory action is not required in this case. The reasons for this are below.

Our consideration of this case

I have investigated whether HMRC has complied with the requirements of data protection legislation.

I understand that there are identity verification checks in place when a Government Gateway account is set up and a Personal Tax Account is created;

[redacted]

Further, I noted that the breach was not reported to the ICO within 72 hours of discovery as required by regulations.

However, in mitigation, we have noted that there is no indication that any of the originating personal data used to commit the fraud was obtained from HMRC.

[redacted]

And whilst HMRC's verification processes are designed to validate identity, safeguards can be passed if someone has genuine customer details. However, if the fraudster attempts to defraud HMRC using those details, there are systems and processes in place to detect and then prevent further attempts to commit fraud.

In terms of what additional information was accessible to the OCG; HMRC advise that gaining access to more personal data via individual-type accounts would require the OCG to initially have more personal data [redacted] the additional personal data available to the criminals was limited.

HMRC advise that any repayments due to genuine customers have been (or will be) made good as part of wider remediation work and therefore all the financial losses will be HMRC's.

HMRC advise that no complaints have been received from any of data subjects affected by the breach. None of the data subjects have reported any direct or indirect losses to HMRC.

Other mitigation action taken by HMRC includes:

- Working with DWP to establish to determine if the access to the DWP UC service on the affected accounts was genuine or not.

- Government Gateway credentials will be deleted to remove access to the affected HMRC accounts as part of remediation. An attempt could be made again by the OCG, but this will be made difficult because of the additional measures HMRC will implement.

- Operational Team carrying out review and remediation of customers' records have taken on and trained additional resource to increase the pace of that work.

- Further remediation work includes:

    - Closing the UTRs and issuing new UTRs.
    - The accounts to be cleansed to how they looked prior to the fraudulent activity.
    - Fraudulent GG accounts which were created will be deleted as appropriate.
    - 130 data subjects who have also been registered for DWP's UC service, currently working to establish if incorrectly registered.

We also welcome the remedial steps taken by HMRC in light of this incident. In particular:

- [redacted]

[redacted] This will increase the protection applied to customer records and data and make attacks of this nature more difficult, and the restrictions on repayments should reduce the incentive for criminals to impersonate customers in this way.

- In parallel a wider piece of HMRC work is underway [redacted] namely:

    - How HMRC verifies the identity of customers across communications channels.
    - How HMRC verifies data presented at the point of registration for tax services.
    - How HMRC identifies and prevents criminal access to customer data.
    - How HMRC repairs the damage resulting from criminal access to customer accounts in a consistent and efficient manner.

Therefore, after careful consideration and based on the information provided, we have decided not to take any formal enforcement action in this case.

Further Action Recommended

The Commissioner considers that HMRC needs to take certain steps to improve compliance with UK GDPR. In particular:

1. HMRC should ensure that breaches which cross the threshold for reporting to the ICO are reported without undelay and within 72 hours of discovery of the breach. HMRC should have measures in place to safeguard this practice.

   There is assistance available in this respect on our website:

   Report a breach | ICO

   Any associated decision-making in this respect should be included in HMRC's personal data breach log.

2. If HMRC have not already done so, it should consider reporting this incident to Action Fraud.

3. Ensure the required remediation work is completed on all the affected data subjects' accounts, including informing the data subjects of the breach (if

you decide not to inform the data subjects, then you should document your decision-making in this respect).

4. Establish with DWP if the access to the DWP's UC service on the affected accounts was genuine or not and take appropriate action if it is found that the access was fraudulent.

5. If HMRC have not already done so, [redacted]

6. HMRC should progress with the programme of works to review and improve HMRC registration processes and repayment controls.

7. Take steps to test the integrity of all the new processes introduced by your organisation as a result of this type of incident.

In addition, I have noted that HMRC are undertaking a wider piece of work [redacted]

Please note that if further information relating to this incident comes to light, or if any further incidents involving HMRC are reported to us, we will revisit this matter, and enforcement action will be considered as a result.

Further information about compliance with the GDPR can be found at the following link.

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the matter closed.

Yours sincerely

Polly Greenwood
Lead Case Officer
Investigations
Information Commissioner's Office
0330 313 1699

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the General Data Protection Regulation, the Data Protection Act 2018

and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

The ICO publishes the outcomes of its investigations. Examples of published data sets can be found at this link (https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/).

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice

Responses to the additional ICO questions, in relation to the

Data Breach Notification on [redacted]

Further information

In order that I may assess this matter and determine what, if any, further action may be necessary, please provide the following information:

Breach

1. Please provide a copy of your internal investigation report in connection with this incident. In the event there is no investigation report, then please provide as much detail as possible as to what happened and how this incident occurred.

The initial investigation into this attack had already identified the source, nature and scale of the attack before the incident was formally raised on HMRC systems. Details of those findings were added to the incident report and shared as necessary. However, it was agreed that a formal investigation report (usually triggered by the incident being formally raised) would not be required as it would add no additional value or information to the earlier investigation.

An Organised Crime Gang (OCG) have used 193 National Insurance Numbers (NINo) to set up bogus Government Gateway accounts [redacted] we are then seeing enrolments on the bogus Government Gateway of genuine Self-Assessment (SA) customer Unique Tax References (UTRs).
This is then followed by the submission of fraudulent 2019/20 returns on genuine customer SA accounts [redacted]
This has resulted in fraudulent expenses claimed relating to these genuine employment details/figures.

2. If not explained in your answer to the previous question, please provide responses to the following:

i. Please confirm the number of data subjects and records affected by the breach.

193

ii. Please confirm if the OCG created new customer accounts, or did it access existing genuine customer accounts, or both. Please provide a breakdown of the numbers involved.

OCG created 193 new PTA using genuine customer data.

iii. It is understood the OCG used hijacked NINOs to set up bogus Government Gateway accounts [redacted] Other than a NINO, was any other personal data used by the OCG to set up the bogus accounts? Please provide full details.

[redacted] See answer to question 2v.

iv. Are HMRC able to confirm if the personal data used by the OCG to access (or create) customer accounts was from an external source (to HMRC)? Or did the personal data in this respect originate from HMRC? Please provide any available information in respect of this aspect.

There is no indication that any personal information was initially obtained or originated directly from HMRC. [redacted]

v. In what way did the OCG [redacted]

[redacted]

vi. Please explain in as much detail as possible how once the OCG had set up the bogus accounts, that it was then then able to access Personal Tax accounts (PTAs) of genuine customers.

Once the OCG have created the Government Gateway account [redacted]

vii. It is understood that the OCG [redacted] please provide full detailed breakdown of the personal data which was obtained by the OCG, including the number of records and data subjects affected by this aspect of the breach.

The 193 PTA accounts created provided access to PAYE Income Summaries, National Insurance information & State Pension data. A subset of 38 accounts were also registered for Income Tax Self-Assessment (ITSA), but the majority of the victims were registered by the OCG, so only the false information provided by the criminal were additionally accessible.

[redacted]

viii. It is understood that there are indications that in some instances the actions of the OCG diverted payments that would have gone to genuine customers. Please confirm if these losses were suffered by HMRC, as opposed to the data subjects. If data subjects suffered financial losses, please provide further details as to the losses suffered and the actions taken by HMRC to mitigate this.

The repayments fall into one of two categories; there were legitimate repayments that should have gone to (but were diverted away from) the genuine customer and there were fraudulently generated repayments that the genuine customer was not entitled to. Any repayments that should have been made to the genuine customer have been (or will be) made good as part of the wider remediation work and therefore all loss will be to HMRC.

In addition, the data subjects have not reported any direct or indirect losses to HMRC. Financial losses suffered were revenue loss by HMRC.

3. It is noted that there has apparently been access to DWP data. Please provide responses to the following:

i. How and in what way was the OCG able to access DWP data.

[redacted]

ii. What DWP data did the OCG have access to; please provide full details, including the number of data subjects and records affected and the type of data compromised.

The DWP UC service was used with 130 of the data subjects' details during the same time frame. Further work is underway to determine if this activity was instigated by the OCG or the genuine customer.

If the access was not genuine, it is not currently known what data will have been accessible and we are liaising with DWP to determine this.

[redacted]

4. Did your organisation's identification verification processes contain adequate fraud prevention measures to prevent fraudulent access to a customer account, or the new registration of a fraudulent customer or account? Please provide any relevant details regarding the measures in place at the time of the breach.

Whilst the verification processes are designed to validate the identity of the caller/user, these safeguards can be passed if someone other than the genuine customer has access to the right details. [redacted]

5. Were there any other measures in place to prevent fraudsters creating new accounts with stolen/hijacked identities, or accessing existing genuine customer accounts?

HMRC has systems which help track fraudster activity, [redacted] Where fraudulent access is identified, credentials that provide access can be suspended.

6. Is your organisation liaising with law enforcement agencies regarding this breach? If yes, please advise which agencies and advise the extent of their involvement.

[redacted]

Data subjects

7. It is understood from the breach report that your organisation has not informed the data subjects about the breach, as the incident did not meet the threshold for communicating it to the data subjects. In relation to this, please provide answers to the following:

i. Please detail why you felt such notification would not be necessary in this instance.

Data subjects were not informed at the time because:

- there was no apparent impact on the data subjects;
- the threat to their rights and freedoms was therefore deemed to be low;

- this is a complex matter, and is taking time to look across all tax regimes for each individual record to assess the actual level of risk on each data subject;
- all cases are being prioritised for review by an Operational Team to consider the impact on the customer and remediate the records as necessary;
- HMRC will contact the customer and make them aware of any impact once it has been defined
- this was an attack on HMRC systems using data subjects' information already held by fraudsters;
- the attack appears to have been intended to defraud HMRC and potentially DWP, but not data subjects.

ii. Please provide an update; has this position changed? If so, please advise how it has changed, and (if applicable) how and when the data subjects have been informed of the breach.

Whilst the detailed analysis has not fully concluded, we have not identified anything to change our original view (articulated at 7i above), but we will still be notifying the data subjects (as per our response articulated at 8 below).

The Operational Team carrying out the review and remediation of these customer records has taken on and trained additional resource to increase the pace of that work. This is the same team that will be reviewing and remediating the customer records attributed to other similar attacks (attacks already notified to ICO).

8. Has an analysis taken place of all the data subjects' records affected by the breach? If so, please provide full details and in particular advise whether any personal data was altered or deleted by the fraudsters, alongside any other information you feel is relevant. If an analysis has not been carried out, then please explain the rationale for not undertaking this work.

The Operational Team are carrying out the review and remediation of these customer records. This review will reveal what information has been altered or deleted and the customers will be notified accordingly and as necessary.

This will include working with DWP to correct any invalid registrations for UC.

9. If not answered in response to the previous question, have any data subjects' records or accounts been rendered inaccurate by the breach? If yes, please provide full details, including how many data subjects' records have been affected and what action HMRC are taken in this respect to correct these records.

Of the 193 data subjects affected by this breach, 38 have had a fraudulent SA Enrolment resulting in a compromised SA account. This had led to the genuine customer account being inaccurate. As stated, the Operational Team are carrying out the review of these customer records and will complete the required remediation as necessary. Remediation includes closing down the Unique Tax Reference (UTR) and issuing a new UTR. The account is

cleansed to how it looked prior to the fraudulent activity. Fraudulent Government Gateway accounts which were created will be deleted as appropriate.

It is possible that 130 data subjects have also been incorrectly registered for UC, which we are currently working to establish.

10. It is noted from your breach report that it was "not yet known" if this breach resulted in a high risk to the data subjects. Please confirm what the current position is. If you have subsequently assessed that the data subjects are at high risk, please provide full details, including any potential or actual harm to the data subjects.

The risk-based assessment made at the time has not yet changed, namely:

- there was no apparent impact on, or risk to, the data subjects;
- the risk of detriment was therefore deemed to be low;
- the attack was intended to defraud HMRC not customers;
- this was an attack on HMRC systems using customer information already held by fraudsters;
- this is a complex matter, and it will take time to look across all tax regimes for each individual record to assess the actual level of risk on each data subject and we will notify the data subjects accordingly at that point.

11. Has your organisation received any complaints from any data subjects affected by the breach? If yes, please provide details and sample extracts (redacted of personal data) from the complaints detailing the harm the data subjects have suffered where applicable.

There are no records of any complaints from customers regarding this attack or the consequences of this attack.

Mitigating action

12. Have the data subjects' accounts or records which have been affected by this breach been secured to prevent the fraudster accessing them again? If so, please confirm the date(s) or date range in which they were secured.

Government Gateway credentials will be deleted to remove access to HMRC digital accounts, as part of the remediation. An attempt could be made again but will be made difficult because of the additional measures explained at 13.

13. Has your organisation taken any other mitigating action to lessen the effects of this breach? If so, please provide any relevant details.

[redacted]

[redacted]

Remedial steps

14. It is noted that [redacted] In relation to this statement, please provide responses to the following:

[redacted]

[redacted]

[redacted]

[redacted] This will increase the protection applied to customer records and data and make attacks of this nature more difficult, and the restrictions on repayments should reduce the incentive for criminals to impersonate customers in this way.

[redacted]

[redacted]

15. [redacted] Has your organisation identified any risk to customers' personal data being compromised before this type of breach is discovered? If yes, please provide details, including any relevant risk assessment undertaken.

[redacted] We recognise that personal data could be compromised before the detection of repayments in those cases, but due to the types of account used in this case, the additional personal data available to the criminals was limited.

16. It is stated that your organisation is [redacted] If not explained in answers to previous questions, please provide responses to the following:

i. [redacted]

This question has been addressed already in response to Q14.

ii. [redacted]

This question has been addressed already in response to Q14.

iii. [redacted]

This question has been addressed already in response to Q14.

17. Please advise of any remedial steps your organisation has taken to prevent a recurrence of such an incident.

In addition to security steps taken at paragraph 14 iv above, [redacted]

- How HMRC verifies the identity of customers across communications channels;
- How HMRC verifies data presented at the point of registration for tax services;
- How HMRC identifies and prevents criminal access to customer data;
- How HMRC repairs the damage resulting from criminal access to customer accounts in a consistent and efficient manner.

[redacted]

Policy and Procedure

18. Do you consider this incident to have breached any of your organisations policies or procedures? If so, please confirm which policies or procedures, and provide either copies or relevant extracts. Please also advise how these policies or procedures were brought to the employee's attention.

HMRC systems were compromised by an organised attack using information already known by the attackers. [redacted] However, there is no evidence that the attack was enabled in any way by a lack of diligence or awareness on behalf of any employees, nor that HMRC security policies and procedures that support and guide employees in their work have been breached.

Information Commissioner's Office

Report a personal data breach

This form is for organisations that have experienced a personal data breach and need to report it to the ICO. **Please do not include any of the personal data involved in the breach when completing this form**. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

You should ensure the information provided is as accurate as possible and supply as much detail as possible.

If you have already spoken to a member of ICO staff about this breach, please give their name:

Report type

- (•) Initial report
- ( ) Follow-up report

(Follow-up reports only) ICO case reference:

Reason for report – after consulting the guidance

- ( ) I consider the incident meets the threshold to report
- ( ) I do not consider the incident meets the threshold to report, however I want you to be aware
- (•) I am unclear whether the incident meets the threshold to report

About the breach

Please describe what happened

An Organised Crime Gang (OCG) have used 160 NINOs to set up bogus Government Gateways [redacted] we are then seeing enrolments on the bogus GG of genuine SA customer UTRs. This is then

followed by the submission of fraudulent 2019/20 returns on genuine customer SA accounts [redacted] This has resulted in fraudulent expenses claimed relating to these genuine employment details/figures.

Please describe how the incident occurred

See above.

How did the organisation discover the breach?

As part of the standard fraud identification activity undertaken by Preventative Risking (PR) team [redacted]

PR have also identified that there has apparently been access to DWP data.

What preventative measures did you have in place?

These are attacks on HMRC systems by fraudsters already in possession of sufficient customer data [redacted] to facilitate fraudulent activity. HMRC is limited in how that can be prevented and relies on subsequent detection to prevent fraudt

Was the breach caused by a cyber incident?

- ○ Yes
- ◉ No
- ○ Don't know

When did the breach happen?

Date: 19-06-2020 Time:

When did you discover the breach?

Date: 02-12-2020 Time:

Categories of personal data included in the breach (tick all that apply)

- ☐ Data revealing racial or ethnic origin
- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Sex life data

- [ ] Sexual orientation data
- [ ] Gender reassignment data
- [ ] Health data
- [x] Basic personal identifiers, eg name, contact details
- [ ] Identification data, eg usernames, passwords
- [x] Economic and financial data, eg credit card numbers, bank details
- [ ] Official documents, eg driving licences
- [ ] Location data, eg coordinates
- [ ] Genetic or biometric data
- [ ] Criminal convictions, offences
- [ ] Other (please give details below)

Number of personal data records concerned?

160 compromised

How many data subjects could be affected?

160

Categories of data subjects affected (tick all that apply)

- [ ] Employees
- [ ] Users
- [ ] Subscribers
- [ ] Students
- [x] Customers or prospective customers
- [ ] Patients
- [ ] Children
- [ ] Vulnerable adults
- [ ] Other (please give details below)

Potential consequences of the breach

This is an attack on HMRC using known information [redacted] This enables fraudulent repayment claims to be made. Whilst there has been no detailed analysis of the customer records, other than that initially performed in the PR team, indications are that, in some instances, the actions of the OCG have diverted payments that would have gone to the genuine customer.

Is the personal data breach likely to result in a high risk to data subjects?

- ○ Yes
- ○ No
- ◉ Not yet known

Please give details

A detailed and in-depth investigation into each compromised record and each customer's circumstances would be required.

(Cyber incidents only) Recovery time

- ○ We have successfully recovered from the incident with all personal data now at the same state it was shortly prior to the incident
- ○ We have determined that we are able to restore all personal data to the same state it was shortly prior to the incident and are in the process of doing this
- ○ We have determined that we are unable to restore the personal data to the same state it was at shortly prior to the incident, ie backups failed, no current backup, backup encrypted etc
- ○ We are not yet able to determine if personal data can be restored to the same state it was shortly prior to the incident

Had the staff member involved in this breach received data protection training in the last two years?

- ○ Yes
- ○ No
- ◉ Don't know

(Initial reports only) If there has been a delay in reporting this breach, please explain why

Confirming the details and extent of the attack before submitting a formal report within HMRC and a slight delay in that formal process when a different reporting platform was used.

Taking action

Describe the actions you have taken, or propose to take, as a result of the breach

[redacted] HMRC actions are currently limited to cleansing these records, identifying others and monitoring the attack.

Have you taken actions to contain the breach? Please describe these remedial actions

HMRC actions are currently limited to cleansing these records, identifying others and monitoring the attack.

Please outline any steps you are taking to prevent a recurrence, and when you expect they will be completed

Security Incident raised, [redacted]

Have you told data subjects about the breach?

- ○ Yes – we have determined it is likely there is a high risk to data subjects so we have communicated this breach to data subjects
- ○ Yes – we have determined that it is unlikely there is a high risk to data subjects, however decided to tell them anyway
- ○ No – but we are planning to because we have determined it is likely there is a high risk to data subjects
- ◉ No – we determined the incident did not meet the threshold for communicating it to data subjects

Have you told, or are you planning to tell any other organisations about the breach?

- ◉ Yes

○ No

○ Don't know

If you answered yes, please specify

HMRC will be contacting DWP as necessary.

About you

Organisation (data controller) name

HM Revenue and Customs

Registration number

Z9034158

If not registered, please give exemption reason

Business sector

Registered organisation address

100 Parliament Street, Westminster, London SW1A 2BQ

Person making this report

In case we need to contact you about this report

Name [redacted]

Email: [redacted]

Phone: [redacted]

Data protection officer

Or the senior person responsible for data protection in your organisation

☐ Same details as above

Name [redacted]

Email: [redacted]

Phone: [redacted]

Sending this form

Initial report
If this is your initial report, please send your completed form to casework@ico.org.uk, with 'Personal data breach notification' in the subject field.

Follow up report
If this is a follow up report, please *reply to the email we sent you*, attaching this completed form to it. (Make sure you leave the subject line as it is – this will ensure your follow-up gets added to your case).

OR, send by post to:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

You should read our guidance to determine what steps you should take.

Based on the information you have provided, we will contact you within seven calendar days to provide information about our next steps. If this is your initial report, we'll give you a case reference number. If we consider the incident is minor or you have indicated that you do not consider it meets the threshold for reporting, you may not receive a response from us.

If your correspondence relates to an existing case, we'll add it to your case for your case officer to consider.

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

For information about what we do with personal data see our privacy notice.