MODULE 3:
DATA BREACH PREPARATION & RESPONSE

From 25 May 2018 Australian businesses of any size may need to comply with the GDPR if they have an establishment in the European Union (EU), if they offer goods and services in the EU, or if they monitor the behaviours of individuals in the EU.

The GDPR includes requirements that resemble those in the Privacy Act 1988, and additional measures that similarly aim to foster transparent information handling practices and business accountability around data handling.

In the lead-up to the commencement of the GDPR requirements, businesses should confirm whether they are covered by the GDPR, and if so, take steps to implement any necessary changes to ensure compliance.

3.1 PART 1 (OAIC)

Data breaches & the Australian Privacy Act

Key points:

- A data breach is an unauthorised access or disclosure of personal information, or loss of personal information.
- Data breaches can have serious consequences, so it is important that entities have robust systems and procedures in place to identify and respond effectively.
- Entities that are regulated by the Privacy Act should be familiar with the requirements of the NDB scheme, which are an extension of their information governance and security obligations.
- A data breach incident may also trigger reporting obligations outside of the Privacy Act.

WHAT IS A DATA BREACH?

A data breach occurs when personal information that an entity holds is subject to unauthorised access or disclosure or is lost.

Personal information is information about an identified individual, or an individual who is reasonably identifiable. Entities should be aware that information that is not about an individual on its own can become personal information when it is combined with other information, if this combination results in an individual becoming 'reasonably identifiable' as a result.

A data breach may be the result of malicious action (by an external or insider party), human error, or a failure in information handling or associated security systems.

Examples of data breaches include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information.
- unauthorised access to personal information by an employee.
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person.
- disclosure of an individual's personal information to a scammer, because of inadequate identity verification procedures.

CONFIDENTIALITY BREACH

Technically, confidentiality is breached every time some who does not need to know, comes to know something. It is not just when the consequences make themselves felt. Breaches of this kind can occur in writing, by oral transmission or by electronic means including eavesdropping.

AVAILABILITY BREACH

A breach of availability can occur through Denial-of-Service attacks where the web server is deluged with requests, or when millions of spam emails overwhelm servers, or a virus spread on a network.

The latter point is a rather formal argument, based on the literal meaning of the word 'breach'. While it is normal to use the term for incidents affecting confidentiality and leading to unwanted disclosure of information, *temporary unavailability of systems or services is not normally defined as a breach*. People prefer to call this an 'incident' (based on terms used in the ITIL framework).

INTEGRITY BREACH

Whenever the integrity of information or its means of storage are violated. It could be through transmission errors, by intentional manipulation, by unintentional handling errors or by the corruption of file content or structure due to electrical, magnetic or other failures.

CONSEQUENCES OF A DATA BREACH

Data breaches can cause harm in multiple ways.

Individuals whose personal information is involved may be at risk of serious harm, whether that is harm to their physical or mental well-being, financial loss, or damage to their reputation.

Examples of such harm include:

- financial fraud including unauthorised credit card transactions or credit fraud
- identity theft causing financial loss or emotional and psychological harm
- family violence

- physical harm or intimidation
- extortion

A data breach can also negatively impact an entity's reputation for privacy protection, and as a result undercut an entity's commercial interests. As shown in the OAIC's long-running national community attitudes to privacy survey, privacy protection contributes to an individual's trust in an entity. 2 If an entity is perceived to be handling personal information contrary to community expectations, individuals may seek out alternative products and services.

An entity can reduce the reputational impact of a data breach by effectively minimising the risk of harm to affected individuals, and by demonstrating accountability in their data breach response. This involves being transparent when a data breach, which is likely to cause serious harm to affected individuals, occurs. Transparency enables individuals to take steps to reduce their risk of harm. It also demonstrates that an entity takes their responsibility to protect personal information seriously, which is integral to building and maintaining trust in an entity's personal information handling capability.

THE AUSTRALIAN PRIVACY PRINCIPLES

The Privacy Act contains 13 Australian Privacy Principles (APPs) listed below that set out entities' obligations for the management of personal information. The APPs are *principles*-based and technologically *neutral*; they outline principles for how personal information is handled and these may be applied across different technologies and uses of personal information over time.

1. APP 1 — Open and transparent management of personal information
2. APP 2 — Anonymity and pseudonymity
3. APP 3 — Collection of solicited personal information.
4. APP 4 — Dealing with unsolicited personal information.
5. APP 5 — Notification of the collection of personal information.
6. APP 6 — Use or disclosure of personal information.
7. APP 7 — Direct marketing.
8. APP 8 — Cross-border disclosure of personal information.
9. APP 9 — Adoption, use or disclosure of government related identifiers.
10. APP 10 — Quality of personal information.
11. APP 11 — Security of personal information.
12. APP 12 — Access to personal information.
13. APP 13 — Correction of personal information

Compliance with the APPs will reduce the risk of a data breach occurring because they ensure that privacy risks are either reduced or removed during the process of personal information handling, including collection, storage, use, disclosure, and destruction of personal information. For example, APP 3 restricts the collection of personal information. APPs 4.3 and 11.2 outline requirements to destroy or de-identify information if it is unsolicited or no longer needed by the entity.

Compliance with these requirements reduces the amount of data that may be exposed because of a breach.

Compliance with the requirement to secure personal information in APP 11 is key to minimising the risk of a data breach.3 APP 11 requires entities to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. The type of steps that are reasonable to protect information will depend on the circumstances of the entity and the risks associated with personal information handled by the entity.

In addition, APP 1 requires entities to take reasonable steps to establish and maintain practices, procedures, and systems to ensure compliance with the APPs.5

THE NOTIFIABLE DATA BREACHES (NDB) SCHEME

This topic was discussed in some detail in Module 2 – mentioned again here for full disclosure.

The NDB scheme in Part IIIC of the Privacy Act requires entities to notify affected individuals and the Commissioner of certain data breaches.

The NDB scheme requires entities to notify individuals and the Commissioner about 'eligible data breaches'. Such a breach occurs when the following criteria are met:

- There is unauthorised access to, or disclosure of personal information held by an entity (or information is lost in circumstances where unauthorised access or disclosure is likely to occur).
- This is likely to result in serious harm to any of the individuals to whom the information relates.
- The entity has been unable to prevent the likely risk of serious harm with remedial action.

Entities must also conduct an assessment if it is not clear if a suspected data breach meets these criteria. The assessment will determine whether the breach is an 'eligible data breach' that triggers notification obligations.

OTHER OBLIGATIONS

Entities may have other obligations outside of those contained in the Privacy Act that relate to personal information protection and responding to a data breach. These may include other data protection obligations under state-based or international data protection laws. Australian businesses may need to comply with the European Union's (EU's) General Data Protection Regulation (GDPR) if they have an establishment in the EU, if they offer goods and services in the EU, or if they monitor the behaviour of individuals in the EU.

For data breaches affecting certain categories of information, other mandatory or voluntary reporting schemes may exist. For example, entities might consider reporting certain breaches to:

- the entity's financial services provider
- police or law enforcement bodies
- the Australian Securities & Investments Commission (ASIC)
- the Australian Prudential Regulation Authority (APRA)
- the Australian Taxation Office (ATO)
- the Australian Transaction Reports and Analysis Centre (AUSTRAC)
- the Australian Cyber Security Centre (ACSC)
- the Australian Digital Health Agency (ADHA)
- the Department of Health
- State or Territory Privacy and Information Commissioners
- professional associations and regulatory bodies
- insurance providers.

Some entities may have additional obligations to report to the Commissioner under the National Cancer Screening Register Act 2016 (NCSR Act) or have different reporting obligations under the My Health Records Act 2012 (My Health Records Act).

Under the NCSR Act, current and former contracted service providers of the National Cancer Screening Register must notify the Secretary of the Department of Health (the Secretary) and the Commissioner if they become aware of unauthorised recording, use or disclosure of personal information included in the Register. The Secretary must also notify the Commissioner of certain data breaches, including potential breaches, in connection with the National Cancer Screening Register. The Secretary must also consult the Information Commissioner about notifying individuals who may be affected. Separately, entities with NCSR Act obligations must consider whether the incident also requires notification under the NDB scheme, as the two schemes operate concurrently. Where the test for both schemes have been met, the entity may make a joint notification to the Commissioner.

WHY DO YOU NEED A DATA BREACH RESPONSE PLAN?

All entities should have a data breach response plan. Your actions in the first 24 hours after discovering a data breach are often crucial to the success of your response. A quick response can substantially decrease the impact on the affected individuals.

High profile data breaches, both in Australia and overseas, highlight the significant disruption caused by a breach of personal information. Research suggests that the cost to an organisation for a data breach can be significant. Implementing a data breach response plan can assist in mitigating these costs.

Having a data breach response plan is part of establishing robust and effective privacy procedures. And having clear roles and responsibilities is part of good privacy governance. A data breach response plan can also help you:

- Meet your obligations under the Privacy Act — an entity must take reasonable steps to protect the personal information that it holds; those reasonable steps may include having a data response plan.
- Protect an important business asset — the personal information of your customers and clients as well as your reputation.
- Deal with adverse media or stakeholder attention from a breach or suspected breach
- Instil public confidence in your capacity to protect personal information by properly responding to the breach.

3.2 PART 2 (OAIC)

PREPARING A DATA BREACH RESPONSE PLAN

Key points

- A quick response to a data breach, based on an up-to-date data breach response plan, is critical to effectively managing a breach
- your data breach response plan should outline your entity's strategy for containing, assessing and managing the incident from start to finish
- this part will provide practical guidance to help you develop a comprehensive and effective data breach response plan.

WHY DO YOU NEED A DATA BREACH RESPONSE PLAN?

All entities should have a data breach response plan. A data breach response plan enables an entity to respond quickly to a data breach. By responding quickly, an entity can substantially decrease the impact of a breach on affected individuals, reduce the costs associated with dealing with a breach, and reduce the potential reputational damage that can result.

A data breach response plan can help you:

MEET YOUR OBLIGATIONS UNDER THE PRIVACY ACT

Under the Privacy Act, an entity must take reasonable steps to protect the personal information that it holds. A data breach response plan focussed on reducing the impact of a breach can be one of these reasonable steps.

LIMIT THE CONSEQUENCES OF A DATA BREACH

A quick response can reduce the likelihood of affected individuals suffering harm. It can also lessen financial or reputational damage to the entity that experienced the breach.

PRESERVE AND BUILD PUBLIC TRUST

An effective data breach response can support consumer and public confidence in an entity's respect for individual privacy, and the entity's ability to manage personal information in accordance with community expectations.

WHAT IS A DATA BREACH RESPONSE PLAN?

A data breach response plan is a framework that sets out the roles and responsibilities involved in managing a data breach. It also describes the steps an entity will take if a data breach occurs.

Your data breach response plan should be in writing to ensure that your staff clearly understand what needs to happen in the event of a data breach. It is also

important for staff to be aware of where they can access the data breach response plan on short notice.

You will need to regularly review and test your plan to make sure it is up to date and that your staff know what actions they are expected to take. You can test your plan by, for example, responding to a hypothetical data breach and reviewing how your response could be made more effective.

How regularly you test your plan will depend on your circumstances, including the size of your entity, the nature of your operations, the possible adverse consequences to an individual if a breach occurs, and the amount and sensitivity of the information you hold. It may be appropriate in some instances that a review of the plan coincides with the introduction of new products, services, system enhancements, or such other events which involve the handling of personal information.

WHAT SHOULD THE PLAN COVER?

The more comprehensive your data breach response plan is, the better prepared your entity will be to effectively reduce the risks and potential damage that can result.

Information that your plan should cover includes:

A CLEAR EXPLANATION OF WHAT CONSTITUTES A DATA BREACH

This will assist your staff in identifying a data breach should one occur (see What is a data breach? section above). You may also want to include potential examples of a data breach which are tailored to reflect your business activities.

A STRATEGY FOR CONTAINING, ASSESSING AND MANAGING DATA BREACHES

This strategy should include the actions your staff, and your response team, will take in the event of a data breach or a suspected data breach. Consider:

- potential strategies for containing and remediating data breaches
- ensuring you have the capability to implement those strategies as a matter of priority (e.g., having staff available to deal with the breach – see Response team membership section below). Your plan should reflect the capabilities of your staff to adequately assess data breaches and their impact, especially when breaches are not escalated to a response team.
- legislative or contractual requirements (such as the requirements of the NDB scheme if they apply to your entity)
- a clear and immediate communications strategy that allows for the prompt notification of affected individuals and other relevant entities. In particular:
  - who is responsible for implementing the communications strategy.

- determining when affected individuals must be notified (refer to Identifying eligible data breaches for further information about mandatory data breach notification requirements under the NDB scheme)
- how affected individuals will be contacted and managed.
- criteria for determining which external stakeholders should be contacted (for example, law enforcement and cyber security agencies, regulators such as the OAIC, and the media)
- who is responsible for liaising with external stakeholders.

THE ROLES AND RESPONSIBILITIES OF STAFF

Your plan should outline the responsibilities of staff members when there is a data breach, or a suspected data breach. Consider:

- who staff should inform immediately if they suspect a data breach
- the circumstances in which a line manager can handle a data breach, and when a data breach must be escalated to the response team. The following factors may determine when a data breach is escalated to the response team:
  - the number of people affected by the breach or suspected breach
  - whether there is a risk of serious harm to affected individuals now or in the future
  - whether the data breach or suspected data breach may indicate a systemic problem with your entity's practices or procedures
  - other issues relevant to your circumstances, such as the value of the data to you or issues of reputational risk.
- who is responsible for deciding whether the breach should be escalated to the response team. One option is for each senior manager to hold responsibility for deciding when to escalate a data breach to the response team. Another option is to have a dedicated role, such as the privacy contact officer.

DOCUMENTATION

Your plan should consider how your entity will record data breach incidents, including those that are not escalated to the response team. This will assist you in ensuring you have documentation of how your entity has met regulatory requirements.

RESPONSE TEAM MEMBERSHIP

Your data breach response team is responsible for carrying out the actions that can reduce the potential impact of a data breach. It is important that the staff that make up the response team, as well as their roles and responsibilities, are clearly established and documented before a data breach occurs. Otherwise, your response to the breach may be unnecessarily delayed.

Who is in your data breach response team will depend on the circumstances of your entity and the nature of the breach. Different skill sets and staff may be needed to respond to one breach compared to another. In some cases, you may need to include external experts in your team, for example legal advice, data forensics, or media management. You should identify the types of expertise you may need and ensure that this expertise will be available on short notice. You might consider creating a core team and adding other members as they are required.

You should keep a current list of response team members and clearly detail their roles, responsibilities, and authorities, as well as their contact details (possibly attached to the data breach response plan). You should ensure these contact details remain updated, particularly in the event of organisational changes. Each role on the response team should have a second point of contact in case the first person is not available.

TYPICAL DATA BREACH RESPONSE TEAM ROLES AND SKILLS

Your data breach response team may include:

- **Team leader** — who is responsible for leading the response team and reporting to senior management.
- **Project manager** — to coordinate the team and provide support to its members.
- **Senior member of staff** with overall accountability for privacy and/or key privacy officer — to bring privacy expertise to the team.
- **Legal support** — to identify legal obligations and provide advice.
- **Risk management support** — to assess the risks from the breach.
- **Information and Communication Technology (ICT) support/forensics support** — this role can help establish the cause and impact of a data breach that involved ICT systems.
- **Information and records management expertise** – to assist in reviewing security and monitoring controls related to the breach (for example, access, authentication, encryption, audit logs) and to provide advice on recording the response to the data breach.
- **Human resources (HR) support** — if the breach was due to the actions of a staff member.
- **Media/communications expertise** — to assist in communicating with affected individuals and dealing with the media and external stakeholders.

If you hold an insurance policy for data breaches, that insurer may have a pre-established panel of external service providers in many of the roles listed above. You may want to consult with your insurer as to the identity of that panel so they can be included in any response team. Alternatively, the insurer may have a hotline available to assist in the event of a data breach, and that could be noted in the response plan.

Which individuals carry out the roles outlined in your response team will depend on your circumstances. For example, in smaller entities it may not be necessary to include steps related to escalating the data breach to the response team, as this may be an automatic process. Depending on the size of your entity or the size of the breach, a single person may perform multiple roles. In smaller entities the owner/principal of the entity could potentially be the person who needs to respond to and act on that breach.

It is important that the response team has the authority to take the steps outlined in the response plan without needing to seek permission, as this will enable a faster response to the breach. The role of team leader should be carefully considered, as they should have sufficient ability and authority to effectively manage the various sections within the entity whose input is required and to report to senior management. It may be your senior member of staff with overall accountability for privacy, a senior lawyer (if you have an internal legal function) or another senior manager. If the breach is serious, it may be a senior executive.

ACTIONS THE RESPONSE TEAM SHOULD TAKE

A data breach response plan should also set out (or refer to) the actions the response team is expected to take when a data breach is discovered. Part 3 of this Guide provides a general framework for responding to a data breach, and Part 4 outlines the requirements of the NDB scheme, which may apply to your entity if they have personal information security obligations under the Privacy Act.

The response team will need to consider what information needs to be reported to senior management and at what point. This reporting structure should form part of the plan.

The data breach response plan should outline how staff will record how they have become aware of a data breach and the actions taken in response. Keeping records on data breaches and suspected breaches will help you manage the breach and identify risks that could make a breach more likely to occur.

OTHER CONSIDERATIONS

In developing your plan, you could also consider:

- when and how the response team could practice a response to a breach to test procedures and refine them
- whether your plan for dealing with personal information data breaches could link into or be incorporated into already existing processes, such as a disaster recovery plan, a cyber security/ICT incident response plan, a crisis management plan or an existing data breach response plan involving other types of information (e.g., commercially confidential information)
- whether senior management should be directly involved in the planning for dealing with data breaches and in responding to serious data breaches

- any reporting obligations under laws other than the Privacy Act or to other entities
- whether you have an insurance policy for data breaches that includes steps you must follow.

DATA BREACH RESPONSE PLAN QUICKCHECKLIST

Use this list to check whether your response plan addresses relevant issues.

Information to be included	Yes/No	Comments
What a data breach is and how staff can identify one		
Clear escalation procedures and reporting lines for suspected data breaches		
Members of the data breach response team, including roles, reporting lines and responsibilities		
Details of any external expertise that should be engaged circumstances		
How the plan will apply to various types of data breaches and varying risk profiles with consideration of possible remedial		
An approach for conducting assessments		
Processes that outline when and how individuals are notified		
Circumstances in which law enforcement, regulators (such as the OAIC), or other entities may need to be contacted		
Processes for responding to incidents that involve another entity		
A record-keeping policy to ensure that breaches are		
Requirements under agreements with third parties such as insurance policies or service agreements		
A strategy identifying and addressing any weaknesses in data handling that contributed to the breach		
Regular reviewing and testing of the plan		
A system for a post-breach review and assessment of the data breach response and the effectiveness of the data breach response		

3.3 PART 3 (OAIC)

RESPONDING TO DATA BREACHES — FOUR KEY STEPS

Key points

- Each data breach response needs to be tailored to the circumstances of the incident.
- In general, a data breach response should follow four key steps: contain, assess, notify and review.

OVERVIEW

Data breaches can be caused or exacerbated by a variety of factors, involve different types of personal information, and give rise to a range of actual or potential harms to individuals and entities.

As such, there is no single way of responding to a data breach. Each breach will need to be dealt with on a case-by-case basis, with an understanding of the risks posed by a breach and the actions that would be most effective in reducing or removing these risks.

Generally, the actions taken following a data breach should follow four key steps:

Step 1: Contain the data breach to prevent any further compromise of personal information.

Step 2: Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.

Step 3: Notify individuals and the Commissioner if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.

Step 4: Review the incident and consider what actions can be taken to prevent future breaches.

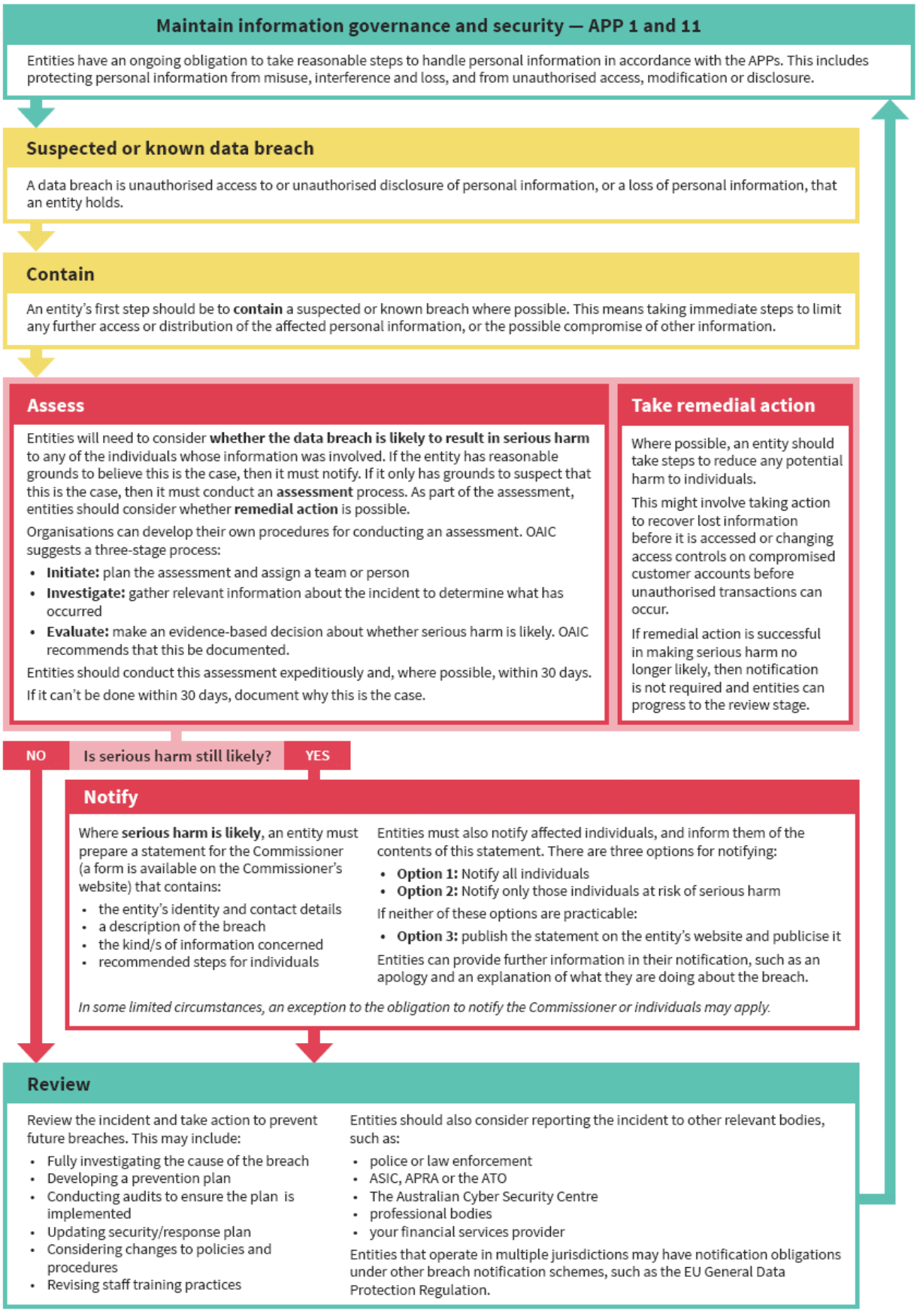
At any time, entities should take remedial action, where possible, to limit the impact of the breach on affected individuals. If remedial action is successful in preventing a likely risk of serious harm to individuals, the NDB scheme notification obligations may not apply.

In general, entities should:

- take each data breach or suspected data breach seriously and move immediately to contain, assess and remediate the incident. Breaches that may initially seem immaterial may be significant when their full implications are assessed

- undertake steps 1 (Contain), 2 (Assess), and 3 (Notify) either simultaneously or in quick succession. In some cases it may be appropriate to notify individuals immediately, before containment or assessment of the breach occurs
- determine how to respond on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, an entity may take additional steps that are specific to the nature of the breach.

The following diagram summarises the data breach response process. The parts of this process that are required by the NDB scheme are coloured red. The NDB scheme is explained in detail in Part 4 of this guide.


Maintain information governance and security — APP 1 and 11
Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.
Suspected or known data breach
A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.
Contain
An entity's first step should be to contain a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.
Assess
Entities will need to consider whether the data breach is likely to result in serious harm to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an assessment process. As part of the assessment, entities should consider whether remedial action is possible.
Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:
Initiate: plan the assessment and assign a team or person
Investigate: gather relevant information about the incident to determine what has occurred
Evaluate: make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.
Entities should conduct this assessment expeditiously and, where possible, within 30 days.
If it can't be done within 30 days, document why this is the case.
Take remedial action
Where possible, an entity should take steps to reduce any potential harm to individuals.
This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.
If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.
NO
Is serious harm still likely?
YES
Notify
Where serious harm is likely, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:
the entity's identity and contact details
a description of the breach
the kind/s of information concerned
recommended steps for individuals
Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:
Option 1: Notify all individuals
Option 2: Notify only those individuals at risk of serious harm
If neither of these options are practicable:
Option 3: publish the statement on the entity's website and publicise it
Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.
In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.
Review
Review the incident and take action to prevent future breaches. This may include:
Fully investigating the cause of the breach
Developing a prevention plan
Conducting audits to ensure the plan is implemented
Updating security/response plan
Considering changes to policies and procedures
Revising staff training practices
Entities should also consider reporting the incident to other relevant bodies, such as:
police or law enforcement
ASIC, APRA or the ATO
The Australian Cyber Security Centre
professional bodies
your financial services provider
Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

STEP 1: CONTAIN

Once an entity has discovered or suspects that a data breach has occurred, it should immediately take action to limit the breach.

For example, stop the unauthorised practice, recover the records, or shut down the system that was breached. If it is not practical to shut down the system, or if it would result in loss of evidence, then revoke or change computer access privileges or address weaknesses in physical or electronic security.

Addressing the following questions may help you identify strategies to contain a data breach:

- How did the data breach occur?
- Is the personal information still being shared, disclosed, or lost without authorisation?
- Who has access to the personal information?
- What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?

At this point, an entity may suspect an eligible data breach under the NDB scheme has occurred, which would trigger assessment obligations. Or the entity may believe the data breach is an eligible data breach, which requires them to notify individuals as soon as practicable.

During this preliminary stage, be careful not to destroy evidence that may be valuable in identifying the cause of the breach, or that would enable the entity to address all risks posed to affected individuals or the entity.

STEP 2: ASSESS

An assessment of the data breach can help an entity understand the risks posed by a data breach and how these risks can be addressed. It should be conducted as expeditiously as possible.

Gather and evaluate as much information about the data breach as possible. By creating a complete picture of the data breach, an entity can ensure they understand the risk of harm to affected individuals and identify and take all appropriate steps to limit the impact of a data breach.

This assessment should also assist entities in deciding whether affected individuals must be notified.

In your assessment of a data breach, consider:

- the type or types of personal information involved in the data breach
- the circumstances of the data breach, including its cause and extent
- the nature of the harm to affected individuals, and if this harm can be removed through remedial action.

All entities should consider whether remedial action can be taken to reduce any potential harm to individuals. This might also take place during Step 1: Contain, such as by recovering lost information before it is accessed.

Entities subject to the NDB scheme are required to assess 'suspected' eligible data breaches and take reasonable steps to complete this assessment within 30 days (see Assessing a suspected data breach). Criteria for assessing a data breach, including the risk of harm and remedial action, is explored in Identifying eligible data breaches.

STEP 3: NOTIFY

Notification can be an important mitigation strategy that has the potential to benefit both the entity and the individuals affected by a data breach. The challenge is to determine when notification is appropriate. Sometimes, notifying individuals can cause undue stress or harm. For example, notifying individuals about a data breach that poses very little or no risk of harm can cause unnecessary anxiety. It can also de-sensitise individuals so that they don't take a notification seriously, even when there is a real risk of serious harm. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required.

Consider:

- the obligations of the entity under the NDB scheme. Entities are required to notify individuals and the Commissioner about data breaches that are likely to result in serious harm. Part 4 of this guide provides further detail about the NDB scheme's requirements
- other circumstances in which individuals should be notified. For example, your entity may not have obligations under the NDB scheme, but have processes in place to notify affected individuals in certain circumstances
- how notification should occur, including:
    - what information is provided in the notification
    - how the notification will be provided to individuals
    - who is responsible for notifying individuals and creating the notification?
- who else other than affected individuals (and the Commissioner if the notification obligations of the NDB scheme apply) should be notified
- where a law enforcement agency is investigating the breach, it may be appropriate to consult the investigating agency before making details of the breach public
- whether the incident triggers reporting obligations to other entities.

Effective data breach response is about reducing or removing harm to affected individuals, while protecting the interests of your organisation or agency. Notification has the practical benefit of providing individuals with the opportunity

to take steps to protect their personal information following a data breach, such as by changing account passwords or being alert to possible scams resulting from the breach. It is important that staff can engage with individuals who have been affected by a data breach with sensitivity and compassion, in order not to exacerbate or cause further harm. Notification can also help build trust in an entity, by demonstrating that privacy protection is taken seriously.

STEP 4: REVIEW

Once steps 1 to 3 have been completed, an entity should review and learn from the data breach incident to improve its personal information handling practices.

This might involve:

- a security review including a root cause analysis of the data breach
- a prevention plan to prevent similar incidents in future
- audits to ensure the prevention plan is implemented
- a review of policies and procedures and changes to reflect the lessons learned from the review
- changes to employee selection and training practices
- a review of service delivery partners that were involved in the breach.

In reviewing information management and data breach response, an entity can refer to the OAIC's

GUIDE TO SECURING PERSONAL INFORMATION

When reviewing a data breach incident, it is important to use the lessons learned to strengthen the entity's personal information security and handling practices, and to reduce the chance of reoccurrence. A data breach should be considered alongside any similar breaches that have occurred in the past, which could indicate a systemic issue with policies or procedures.

If any updates are made following a review, staff should be trained in any changes to relevant policies and procedures to ensure a quick response to a data breach.

3.4 PART 4: (OAIC)

NOTIFIABLE DATA BREACH (NDB) SCHEME

The Privacy Act requires certain entities to notify individuals and the Commissioner about data breaches that are likely to cause serious harm.

The requirements of the NDB scheme are contained in Part IIIC of the Privacy Act and apply to breaches that occur on or after 22 February 2018.

This part of the guide covers the following topics:

- Entities covered by the NDB scheme.
- Data breaches involving more than one entity.
- Identifying eligible data breaches
- Exceptions to the notification obligation
- Assessing a suspected data breach
- Notifying individuals about an eligible data breach
- What to include in an eligible data breach statement
- The Australian Information Commissioner's role in the NDB scheme.

ENTITIES COVERED BY THE NDB SCHEME

Key points:

- Entities that have existing obligations under the Privacy Act to secure personal information must comply with the NDB scheme.
- This includes Australian Government agencies, businesses and not-for profit organisations that have an annual turnover of more than AU$3 million, private sector health service providers, credit reporting bodies, credit providers, entities that trade in personal information and tax file number (TFN) recipients.
- Entities that have Privacy Act security obligations in relation to types of information only (for example, small businesses that are required to secure tax file number information) do not need to notify about data breaches that affect other types of information outside the scope of their obligations under the Privacy Act.

AUSTRALIAN PRIVACY PRINCIPLES ENTITIES

The NDB scheme applies to entities that have an obligation under APP 11 of the Privacy Act to protect the personal information they hold (s 26WE(1)(a)).11 Collectively known as ‘APP entities’, these include Australian Government agencies and private sector and not-for-profit organisations with an annual turnover of more than $3 million. The definition of APP entity generally does not include small business operators, registered political parties, state or territory authorities, or a prescribed instrumentality of a state (s 6C). However, some businesses of any size are APP entities, including businesses that trade in personal

information12 and organisations that provide a health service to, and hold health information about, individuals (see Is my organisation a health service provider?).

For more information about APP entities, see Chapter B of the Australian Privacy Principal Guidelines (APP Guidelines).

Exempt acts and practices, including employee records.

The NDB scheme only applies to entities and personal information holdings that are already subject to security requirements under the Privacy Act. This means that acts and practices of APP entities that are exempt from the Privacy Act will also be exempt from the NDB scheme.

For example, in some circumstances, private sector employers do not have to comply with the APPs in relation to employee records associated with current and former employment relationships (s 7B(3)). If an exempt employee record is subject to unauthorised access, disclosure or loss, the private sector employer does not have to assess the breach or notify individuals and the Commissioner. This exemption does not apply to TFN information that is contained within an employee record. However, given community expectations around the handling of their personal information, it is recommended that employers notify affected individuals where a breach of an employee record is likely to result in serious harm. Doing so will enable affected individuals to take protective action against any potential harms, as well as illustrating to employees that the security of their records is taken seriously.

Further information about acts and practices that are exempt from the APPs and, by extension, the NDB scheme can be found in Privacy business resource 13: Application of the Australian Privacy Principles to the private sector.

SMALL BUSINESS OPERATORS

A small business operator (SBO) is an individual (including a sole trader), body corporate, partnership, unincorporated association, or trust that has not had an annual turnover of more than $3 million in any financial year since 2001 (s 6D).

Generally, SBOs (Small Business Operator) do not have obligations under the APPs unless an exception applies (s 6D(4)).

In certain circumstances an SBO must comply with the APPs, and therefore with the NDB scheme. That will be the case where the SBO:

- holds health information and provides a health service
- is related to an APP entity
- trades in personal information. That is, the SBO discloses personal information about individuals to anyone else for a benefit, service or advantage; or provides a benefit, service or advantage through the

collection of personal information about another individual from anyone else
- are a credit reporting bodies
- is an employee association registered under the Fair Work (Registered Organisations) Act 2009
- has 'opted-in' to APP coverage under s 6EA of the Privacy Act.

If an SBO carries on certain activities it must comply with the APPs, and therefore must comply with the NDB scheme, but only in relation to personal information held by the entity for the purpose of, or in connection with, those activities. Those activities include:

- providing services to the Commonwealth under a contract
- operating a residential tenancy data base
- reporting under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006
- conducting a protected action ballot
- information retained under the mandatory data retention scheme, as per Part 5-1A of the Telecommunications (Interception and Access) Act 1979.

More information about how to determine whether a business or organisation is an APP entity or subject to the APPs for some of its activities is available at Privacy business resource 10: Does my small business need to comply with the Privacy Act?.16

CREDIT REPORTING BODIES

A credit reporting body (CRB) is a business or undertaking that involves collecting, holding, using, or disclosing personal information about individuals for the purpose of providing an entity with information about the credit worthiness of an individual (s 6P). Credit reporting information is defined as credit information or CRB derived information about an individual (s 6(1)).

CRBs (Credit Reporting Body) have obligations under the NDB scheme in relation to their handling of credit reporting information (s 26WE(1)(b)), and in relation to their handling of any other personal information for which they have obligations under APP 11.

CREDIT PROVIDERS

The NDB scheme applies to all credit providers whether they are APP entities. The section of the Privacy Act under which a credit provider is required to comply with the scheme will depend on what kind of information is involved in the data breach.

If it is 'credit eligibility information' (defined in s 6(1)) the NDB scheme will apply because of the security requirement in s 21S (1) in relation to that information.

If the credit provider is also an APP entity the NDB scheme applies in relation to other personal information because of the security requirement in APP 11.

The organisations that are credit providers for the purposes of the Privacy Act (s 6G) are:

- a bank
- an organisation or small business operator if a substantial part of its business is the provision of credit, such as a building society, finance company or a credit union
- a retailer that issues credit cards in connection with the sale of goods or services
- an organisation or SBO that supplies goods and services where payment is deferred for seven days or more, such as telecommunications carriers, and energy and water utilities
- certain organisations or SBOs that provide credit in connection with the hiring, leasing, or renting of goods.

An organisation or SBO that acquires the right of a credit provider in relation to the repayment of an amount of credit is also considered a credit provider, but only in relation to that credit (s 6K).

For more information about categories of credit-related personal information, see Privacy business resource 3: Credit reporting – what has changed.

TFN RECIPIENTS

The NDB scheme applies to TFN recipients18 in relation to their handling of TFN information (s 26WE(1)(d)). A TFN recipient is any person who is in possession or control of a record that contains TFN information (s 11). TFN information is information that connects a TFN with the identity of a particular individual (s 6).

A TFN recipient may also be an APP entity or credit provider. In certain circumstances, entities that are not otherwise covered by the Privacy Act, such as state and local government bodies, may also be authorised to receive TFN information and will be considered TFN recipients.

The NDB scheme applies to TFN recipients to the extent that TFN information is involved in a data breach. If TFN information is not involved, a TFN recipient would only need to comply with the NDB scheme for breaches of other types of information if they are also a credit provider or APP entity.

More information about TFN recipients is available in Privacy business resource 12: The Privacy (Tax File Number) Rule 2015 and the protection of tax file number information.19

Overseas activities

ENTITIES WITH AN 'AUSTRALIAN LINK'

The NDB scheme generally extends to the overseas activities of an Australian Government agency (s 5B (1)). It also applies to organisations (including small businesses covered by the Act, outlined above) that have an 'Australian link' (s 5B (2)).

An organisation has an Australian link either because it is, in summary, incorporated or formed in Australia (see s 5B(1A) for more detail), or where:

- it carries on business in Australia or an external Territory, and
- it collected or held personal information in Australia or an external Australian Territory, either before or at the time of the act or practice (s 5B (3)).

Further information about entities that are taken to have an Australian link is available in Chapter B of the APP Guidelines.

Disclosing personal information overseas

If an APP entity discloses personal information to an overseas recipient, in line with the requirements of APP 8.1, then the APP entity is deemed to 'hold' the information for the purposes of the NDB scheme (s 26WC (1)). APP 8.1 says that an APP entity that discloses personal information to an overseas recipient is required to take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information. This means that if the personal information held by the overseas recipient is subject to loss, unauthorised access, or disclosure, the APP entity is still responsible for assessing whether it is an eligible data breach under the Privacy Act, and if it is, for notifying individuals at risk of serious harm and providing a statement to the Commissioner.

There are exceptions to the requirement in APP 8.1 to take reasonable steps. APP entities that disclose information overseas under an exception in APP 8.2 are not taken to 'hold' information they have disclosed overseas under s 26WC. In these circumstances, if the personal information held by the overseas recipient is subject to a data breach, the APP entity does not have obligations to notify about the breach under the NDB scheme.

More information about APP 8 is available in Privacy business resource 8: Sending personal information overseas.21

Disclosing credit eligibility information

If a credit provider discloses credit eligibility information about one or more individuals to a person, a body or a related body corporate that does not have an 'Australian link' (s 26WC(2)(a)), the credit provider may also have obligations under the NDB scheme in respect of that information. If credit eligibility information held by the person or related body corporate is subject to loss, unauthorised access, or disclosure, the credit provider is responsible for assessing

whether there is an eligible data breach that needs to be notified to individuals at risk of serious harm and the Commissioner.

3.5 CASE STUDY: EQUIFAX DATA BREACH

In July 2017, credit reporting agency Equifax were the victims of a significant data breach which resulted in an estimated 143 million U.S. records containing customer information being stolen by hackers. This included social security numbers, dates of birth, and the credit card details of over 209,000 Americans. The breach also impacted other countries, with Equifax admitting that 15.2 million records of British citizens and 8000 Canadians were stolen in the breach. There was over a month's delay in disclosing the data breach. Senior executives were criticized for selling shares in the days before the breach was announced to the public.

The intruders managed to gain access to the records using a weakness in a popular back-end website application. The vulnerability was made public in March 2017, but Equifax were slow to fix the bug in their networks, highlighting the importance of maintaining the latest patches.

The Equifax hack had the markings of a sophisticated cyber-attack, leading to speculation about attribution, with some in the cyber security community blaming Chinese-backed groups due to similarities with other attacks such as the U.S. Office of Personnel hack in 2017.

The potential for the stolen Equifax data to be used in financial fraud has caused U.S. banks such as Citi Group and Wells Fargo to step up anti-fraud controls.