*Australian Government Solicitor*

# SUMMARY REPORT

## PRIVACY BREACH INVESTIGATION

## Investigation into Privacy Breach – ASIC Connect Online Search Retrieval Service

## Australian Securities and Investments Commission

*13 February 2018*

Australian Government Solicitor
ABN 69 405 937 639
Level 34, 600 Bourke Street
Melbourne VIC 3000

www.ags.gov.au

**CONTENTS**

**SUMMARY REPORT**

**PRIVACY INVESTIGATION – ASIC REGISTRY PRIVACY BREACH**

## 1. EXECUTIVE SUMMARY

1.1. On 9 November 2017, the Australian Securities and Investment Commission (**ASIC**) notified the Office of the Australian Information Commissioner (**OAIC**) of a privacy breach connected with its Search Retrieval Service (**the Service**).

1.2. The Service enabled a person to retrieve the details of previous purchases of extracts and lodged documents from ASIC's registers and to view the purchased search products. A search could be conducted against any email address to view purchases made in the last 90 days.

### SCOPE OF THE INVESTIGATION

1.3. On 5 December 2017, AGS received a work order to conduct an investigation of the approval, design and implementation of the Service, as well as the adequacy of ASIC's response and procedures following receipt of the complaint on 27 October 2017.

1.4. AGS was also asked to consider the steps taken (and any further steps required) by ASIC to identify and notify persons that could have been affected by the breach.

1.5. AGS provided its full report on 1 February 2018. This is a summary of that report containing the full executive summary; all recommendations; and the findings which explain those recommendations. The appendices and some background and minor observations have been removed for ease of reading and to protect the privacy of third parties. This summary faithfully reproduces the key findings in the full report.

### CONCLUSIONS

1.6. AGS has identified a number of opportunities for ASIC to update or implement new policies or processes in response to the privacy breach. In particular, AGS has recommended additional privacy training in a number of areas.

1.7. AGS found the main cause of the breach was inadequate consideration of privacy issues during the design phase. This included failures to follow ASIC's own internal mechanisms for approving new programs.

1.8. There was a period after the breach was reported where ASIC staff did not adequately progress it as a privacy issue. In part this was because key staff did not recognise the privacy issue in the complaint.

1.9. Once the incident was recognised as a privacy breach and referred to the privacy team, ASIC moved reasonably quickly to respond. Efforts to identify affected individuals were frustrated by a lack of audit log for historical access to the system. Taking that into account, AGS considers ASIC's response was proactive once the privacy issue was identified, and as effective as the available information allowed.

The steps that were taken, including notifications, were proportionate to the risks identified.

1.10. Feedback from notified individuals has been positive, reflecting appreciation for ASIC's efforts to mitigate risk. There have been no reports suggesting actual harm occurred to any affected individual. Statistical analysis of the nil result searches does not indicate 'phishing' has occurred on any coordinated scale.

1.11. The analysis in Parts 1 to 3 of this Report includes 28 recommendations as to improvements to policies, procedures and training. **Table 1** below provides an overview of the key issues and recommendations.

1.12. AGS does not recommend any further restorative steps in connection with the incident itself. At this stage AGS considers ASIC has done all it reasonably can to address the incident. AGS's recommendations are directed at systemic improvements which should lessen the risk of a similar incident occurring again, and improving the likelihood of any future privacy issues being identified as such more quickly.

**ATTRIBUTION AND KEY CONTACTS**

1.13. This report was prepared by the following team. Please contact us if you would like to discuss its contents or if we can do anything further to assist you in this matter.


**Justin Davidson**
Senior Executive Lawyer
T 02 6253 7240
justin.davidson@ags.gov.au

**Molly Scanlon**
Lawyer

**Melissa Gangemi**
Senior Lawyer

**TABLE 1 – RECOMMENDATIONS**

| **Recommendation 1 - Update the *Managing Enhancement Governance* procedure** | |
|---|---|
| ASIC update the *MEG* procedure to require staff to:<br>(1) Identify at Step 1 in the opportunity identification form if the proposed change may impact how personal information is handled<br>(2) For any impacts identified at Step 1, undertake a threshold assessment of privacy risks at Step 2 when completing the Impact Assessment to identify any privacy risk.<br>(3) Assess any potential privacy impacts before the Business Requirements have been approved at Step 3.8 to ensure that the requirements comply with the *Privacy Act 1988*. This assessment should meet at least the minimum standards for a PIA mandated by the OAIC.<br>(4) Require confirmation when creating the TickIT at Step 3.10 that an assessment of privacy risk has occurred.<br>(5) Require confirmation when presenting to the enhancement group that the business requirements have been assessed for privacy risk.<br>(6) Assess any potential privacy impacts during User Acceptance Testing (UAT). Update the UAT Business System Owner (SES or delegate) signoff to include an assessment that the final product compliance with the *Privacy Act 1988*. Where a PIA was previously completed, this requirement could be met by preparing an updated PIA. This assessment should meet at least the minimum standards for a PIA mandated by the OAIC. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 2 – Ensure privacy risks assessed as part of any system change** | |
| ASIC review existing policies relating to system changes to ensure that:<br>(1) potential privacy impacts are considered in a preliminary way whenever personal information is being affected<br>(2) where that preliminary inquiry identifies a substantial change which is likely to impact on privacy interests, a full Privacy Impact Assessment consistent with OAIC policies should be undertaken. | |
| **ASIC Response:** | Agreed. |

| | |
|---|---|
| **Recommendation 3 – Ensure adherence with MEG procedure** | |
| ASIC staff with leadership on MEG procedure to enhance cultural valuing of, and adherence to, MEG procedure. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 4 – SOS staff privacy training** | |
| ASIC implement specific staff training for the SOS team and other staff in similar roles on the nature of personal information, managing privacy risks and the steps to take to escalate or obtain advice on privacy issues and concerns. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 5 – Update IT policies and procedures** | |
| ASIC update the existing IT change policies and procedures to ensure any changes to the business requirements are referred back to the business for an assessment of potential privacy risk arising from the changes.<br><br>Assess any potential privacy impacts during User Acceptance Testing (UAT). Update the UAT Business System Owner (SES or delegate) signoff to include an assessment that the final product compliance with the *Privacy Act 1988*. This assessment should meet at least the minimum standards for a Privacy Impact Assessment mandated by the OAIC. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 6 – IT staff privacy training** | |
| ASIC implement specific staff training for the IT team on identifying and managing privacy risks and the steps to take to escalate or obtain advice on privacy issues and concerns. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 7 – ASIC train staff to immediately raise privacy concerns** | |
| ASIC train staff to implement an organisation wide practice to immediately raise any privacy concerns with a supervisor, so that they may be escalated as required. | |
| **ASIC Response:** | Agreed. |

| | |
|---|---|
| **Recommendation 8 – ASIC undertake regular checks of privacy links** | |
| ASIC undertake regular checks of privacy links. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 9 – ASIC add a link to CAA privacy page to its privacy policy** | |
| ASIC add a link to the webpage titled ‘complaints about our handling of your privacy’ in the CAA section of its website to its privacy policy. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 10 – ASIC train staff to lodge privacy complaints** | |
| ASIC train staff to ensure complaints made other than via the CAA are nonetheless appropriately progressed internally, and where there is doubt to clarify with an individual raising concerns whether they wish to lodge a privacy complaint. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 11 – All privacy CAA be referred to CLO for assessment** | |
| ASIC ensure that all complaints raising privacy issues or concerns be brought to the attention of the privacy team within the CLO for assessment on whether CLO should be involved. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 12 – CLO Complaints Officer training** | |
| ASIC implement specific training for CLO Complaints Officers on identification of potential privacy issues in complaints, and the process for referring issues for assessment by the privacy team. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 13 – CLO undertake prelim assessment of privacy complaints** | |
| A preliminary risk assessment of any complaint raising privacy issues be undertaken by, or in conjunction with, a member of the privacy team. | |
| **ASIC Response:** | Agreed. |

| | |
|---|---|
| **Recommendation 14 – Privacy team training regarding handling privacy complaints** | |
| ASIC train privacy team staff to handle privacy complaints, including undertaking preliminary assessments. ASIC ensure that lawyers undertaking such assessments have appropriate knowledge of privacy issues, as well as ASIC policies and procedures. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 15 – Implementation of a data breach response plan** | |
| (a) ASIC finalise and implement a data breach response plan, including the appointment of a data breach response team.<br>(b) ASIC train the data breach response team to implement the data breach response plan.<br>(c) ASIC update its Complaints Guidance to reflect that ASIC will respond to suspected or actual privacy breaches in accordance with its data breach response plan. | |
| **ASIC Response:** | Agreed. This recommendation is already in progress. |
| **Recommendation 16 – Continued development of privacy resources** | |
| ASIC develop privacy resources, including a manual to guide handling of personal information, to be published on the privacy resource page on its intranet. | |
| **ASIC Response:** | Agreed. Already in progress. |
| **Recommendation 17 – ASIC update induction and annual staff training** | |
| ASIC review its induction and annual privacy training to ensure that staff are trained to effectively identify and report privacy concerns, have knowledge of the data breach response plan and can locate key privacy resources. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 18 – Legal officer training** | |
| ASIC implement specific training for legal officers outside CLO, or at a minimum, the privacy champion for each non-CLO legal team, on identification of potential privacy issues, the process for referring issues for assessment by the privacy team, and the implementation of the data breach response plan. | |
| **ASIC Response:** | Agreed. |

| | |
|---|---|
| **Recommendation 19 – CCC staff training, quality assurance and supervision** | |
| (a) ASIC continue to deliver tailored training to CCC staff.<br>(b) ASIC undertake quality assurance assessment to ensure that call centre staff are able to receive calls and adequately address issues before commencing work.<br>(c) ASIC ensure CSOs are trained to raise concerns with other staff, including their supervisor, floor walkers, performance coaches and the helpdesk, where their supervisor is unavailable. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 20 – ASIC take immediate steps to contain potential breaches** | |
| The ASIC data breach response plan provide that immediate steps should be taken to contain any actual or suspected privacy breach (regardless of whether a full assessment of the suspected breach has been carried out). | |
| **ASIC Response:** | Agreed. Already in progress. |
| **Recommendation 21 – ASIC undertake PIA before Service recommences** | |
| ASIC undertake a PIA on the Service, as amended, before it recommences operation. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 22 – All handling of personal information to be recorded in logs** | |
| ASIC develop a risk based approach to ensure where appropriate the handling of all personal information by new and existing systems be recorded in an audit log. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 23 – ASIC review the storage period of all audit logs** | |
| ASIC review the storage period of all audit logs and ensure retention periods are adequate based on the nature of the service, types of information handled and the potential risk of harm if misuse occurs. | |
| **ASIC Response:** | Agreed. Since 2016 all new systems have been built in compliance with the Record retention requirements under the National Archives Act. |

| | |
|---|---|
| **Recommendation 24 – ASIC review risk and guard against phishing** | |
| ASIC ensure that in any reboot of the Service, IT consider implementing systems solutions that enable ASIC to detect and respond to any suspected phishing through the Service. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 25 – ASIC privacy training cover potential harm from breaches** | |
| ASIC privacy training cover the potential consequences of a privacy breach, including potential harm to individuals and to the agency. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 26 – Privacy team training re Notifiable Data Breach scheme** | |
| ASIC ensure privacy team staff receiving training regarding the Notifiable Data Breaches scheme | |
| **ASIC Response:** | Agreed. |
| **Recommendation 27 – Privacy team training on preparation of data breach notices** | |
| ASIC ensure that privacy team staff are trained on the preparation of data breach notices with reference to lessons learned from this incident. | |
| **ASIC Response:** | Agreed. |
| **Recommendation 28 – ASIC consider review of Registry system upgrades** | |
| ASIC should undertake a risk-based assessment of Registry system upgrades involving handling personal information where no assessment of potential privacy impacts was undertaken. | |
| **ASIC Response:** | Agreed. |

## 2. BACKGROUND

2.1. On 9 November 2017, the Australian Securities and Investment Commission (**ASIC**) notified the Office of the Australian Information Commissioner (**OAIC**) of a privacy breach connected with its Search Retrieval Service (**the Service**).

2.2. ASIC administers 31 statutory registers which can be searched by the public directly through ASIC's online search service called 'ASIC Connect'. Some of the searches through ASIC attract a fee, but all data is otherwise publically available. In order to request a paid search, a user must enter an email address to which the purchased product and a receipt are sent after the credit card transaction is made. ASIC retains the email address for each paid search for a period of 90 days.

### Search Retrieval Service

2.3. The Service was intended to work as follows:

2.3.1. A user would enter an email address or the receipt number for a paid search. If an email address was entered, the user could enter a date range of up to 90 days prior to the retrieval date.

2.3.2. The service then displayed details of paid searches being the receipt number, the date of purchase, the entity name related to the extract, the product type and the amount paid.

2.3.3. A user could select a previous paid search that would then display the additional information of the type of credit card used for the transaction and options to view the payment receipt, view or download each product purchased and resend the receipt and products purchased to an email address. Information including the information provided to make the purchase (such as a credit card number) was not displayed.

2.3.4. If no result was found (**nil result**) then the user would be notified that no previous search was found on a new screen because either the purchase was undertaken more than 90 days ago or because the email address entered was incorrect.

2.4. If the user chose to resend the receipt and products to an email address, the user could enter a different email address. ASIC would keep a record of this email address for 132 days.

2.5. As discovered on 9 November 2017, there were privacy issues which arose out of the implementation of the Service. Specifically, we identify those issues as follows:

2.5.1. users could enter any known individual's email address and a general date range without further validation to receive a search history

2.5.2. users could then view the nature, details and dates of previous paid searches for that email address in the past 90 days

2.5.3. users could also resend to any email address the purchased extracts or documents

2.5.4. users could view and resend to an email address details of the purchase including receipt number, payment amount and payment method

2.5.5. users could also view when an individual's email address had not been used to purchase any products in the previous 90 days.

**Scope of the AGS investigation**

2.6. On 5 December 2017, AGS received a work order to conduct an investigation into the approval, design and implementation of the Service, including a:

2.6.1. review of the security requirements, tests and approvals as required in ASIC policies and procedures

2.6.2. review of any PIA or other privacy assessment undertaken

2.6.3. review of the testing and implementation of the service.

2.7. As part of its investigation, AGS was also instructed to:

2.7.1. investigate the adequacy of ASIC's response and procedures following receipt of the complaint on 27 October 2017

2.7.2. consider the steps taken (and any further steps required) by ASIC to identify and notify persons that could have been affected by the breach

2.7.3. make recommendations for improvements to policies and procedures.

2.8. Separate to this investigation, ASIC have requested AGS's assistance to prepare a draft Data Response Plan, review its Privacy Policy and prepare a privacy manual for ASIC staff.

2.9. The investigation has been completed through meeting with relevant ASIC staff and a desktop review of relevant documents. AGS also consulted directly with members of the ASIC Chief Legal Office (CLO) Privacy team on key issues.

## 3. PART 1: APPROVAL, DESIGN AND IMPLEMENTATION OF THE SERVICE

### Process review – Managing Enhancement Governance procedure

3.1. The Systems and On-line Services (**SOS**) team[1] is responsible for designing any enhancements which are implemented by IT on Registry's instructions.

3.2. Enhancements are implemented in accordance with the *Managing Enhancement Governance* (**MEG**) procedure.

3.3. Privacy is not mentioned in the MEG procedure, and the document is silent on the potential for a system enhancement to pose a privacy risk.

3.4. Although the process requires staff to identify any legislative restraints, it does not directly ask staff to consider if the change will involve personal information or any changes to the handling of personal information such that it might be restrained by the *Privacy Act 1988*. To guard against the risk of issues not being seen as 'privacy' issues (see recommendation 4), the MEG procedure should describe the issue in non-technical terms eg 'Will information about any individual be used, moved or disclosed?'

3.5. To ensure protections for personal information are in-built into any Registry system enhancement, we recommend that the MEG procedure be updated as follows:

| **Recommendation 1 - Update the *Managing Enhancement Governance* procedure** |
|---|
| ASIC update the *MEG* procedure to require staff to:<br>(7) Identify at Step 1 in the opportunity identification form if the proposed change may impact how personal information is handled<br>(8) For any impacts identified at Step 1, undertake a threshold assessment of privacy risks at Step 2 when completing the Impact Assessment to identify any privacy risk.<br>(9) Assess any potential privacy impacts before the Business Requirements have been approved at Step 3.8 to ensure that the requirements comply with the *Privacy Act 1988*. This assessment should meet at least the minimum standards for a PIA mandated by the OAIC.<br>(10) Require confirmation when creating the TickIT at Step 3.10 that an assessment of privacy risk has occurred.<br>(11) Require confirmation when presenting to the enhancement group that the business requirements have been assessed for privacy risk.<br>(12) Assess any potential privacy impacts during User Acceptance Testing (UAT). Update the UAT Business System Owner (SES or delegate) signoff to include an assessment that the final product compliance with the *Privacy Act 1988*. Where a PIA was previously completed, this requirement could be met by preparing an |

[1] The SOS is comprised of 5 business analysts. The team reports to the Senior Manager, Customer Contact Centre.

| | |
|---|---|
| updated PIA. This assessment should meet at least the minimum standards for a PIA mandated by the OAIC. | |
| **ASIC Response:** | Agreed. |

3.6. We further recommend that ASIC review existing system enhancement policies and procedures (not just in IT) to ensure that an inquiry into potential privacy impacts is undertaken wherever personal information is being affected (eg used, moved or disclosed). Wherever that initial inquiry identifies a substantial change which is likely to impact on privacy interests, a full Privacy Impact Assessment consistent with OAIC policies should be undertaken.

| **Recommendation 2 – Ensure privacy risks assessed as part of any system change** | |
|---|---|
| ASIC review existing policies relating to system changes to ensure that:<br>(3) potential privacy impacts are considered in a preliminary way whenever personal information is being affected<br>(4) where that preliminary inquiry identifies a substantial change which is likely to impact on privacy interests, a full Privacy Impact Assessment consistent with OAIC policies should be undertaken. | |
| **ASIC Response:** | Agreed. |

3.7. After being provided with a draft of this report, ASIC Registry advised that it has commenced steps to update its system change procedures to require staff to review and approve requests associated with policy, legal, risk, data and privacy. In addition, the decision-making register will be updated to reference relevant consultations to inform the decision-maker.

### Implementation review – Search Retrieval Service change

3.8. We identified discrepancies between the MEG procedure and the implementation of the change.

3.9. We consider that the failure to adhere to the MEG procedure significantly increased the risk that a system change would be developed that did not take into account all relevant risks.

| **Recommendation 3 – Ensure adherence with MEG procedure** | |
|---|---|
| ASIC staff with leadership on MEG procedure to enhance cultural valuing of, and adherence to, MEG procedure. | |
| **ASIC Response:** | Agreed. |

3.10. A contributing factor at all stages of managing this issue was the misconception that the upgrade did not handle personal information in an unauthorised way.

3.11. Although the publication of information in ASIC registers is authorised by law, it was not perceived that information about the products purchased by an individual (identifiable by their email address) is personal information. Because of the way the process unfolded, ASIC staff with the requisite knowledge to identify the issue were not sufficiently engaged on the issue. This then exposed a knowledge gap for other parts of the business, which suggests greater awareness of the scope of 'personal information' within a broader ASIC cohort as a future risk mitigation strategy.

| **Recommendation 4 – SOS staff privacy training** | |
|---|---|
| ASIC implement specific staff training for the SOS team and other staff in similar roles on the nature of personal information, managing privacy risks and the steps to take to escalate or obtain advice on privacy issues and concerns. | |
| **ASIC Response:** | Agreed. |

**Process review – IT change processes and policies**

3.12. For completeness, we note that ASIC have provided AGS with a copy of the relevant IT processes and policies which guided the system change.

3.13. Although the Change and Release Policy provides for an assessment of risk, AGS was informed that this is only an assessment of technical risk. It is presumed that any assessment of other risks, such as privacy risk, will be undertaken by the business area before a TickIT is raised to design and implement the system change.

3.14. While we agree that any privacy impact assessment is best carried out at the business requirements stage, we consider that IT should ensure that system change only proceed where privacy risks have already been considered and assessed.

3.15. We further suggest that IT staff be trained to identify and raise any privacy concerns they might have as part of the development and testing of the system change, and liaise with the business area to undertake further assessment of potential privacy impacts should the end solution differ from the approved business rules. Referral back to the business area for further assessment should be incorporated into existing IT change policies and procedures.

| **Recommendation 5 – Update IT policies and procedures** |
|---|
| ASIC update the existing IT change policies and procedures to ensure any changes to the business requirements are referred back to the business for an assessment of potential privacy risk arising from the changes.<br><br>Assess any potential privacy impacts during User Acceptance Testing (UAT). Update the UAT Business System Owner (SES or delegate) signoff to include an assessment that the |

| | |
|---|---|
| final product compliance with the *Privacy Act 1988*. This assessment should meet at least the minimum standards for a Privacy Impact Assessment mandated by the OAIC. | |
| **ASIC Response:** | Agreed. |

| **Recommendation 6 – IT staff privacy training** | |
|---|---|
| ASIC implement specific staff training for the IT team on identifying and managing privacy risks and the steps to take to escalate or obtain advice on privacy issues and concerns. | |
| **ASIC Response:** | Agreed. |

## 4. PART 2: ASIC'S RESPONSE TO THE COMPLAINT

### Implementation review – Handling of 27 October 2017 complaint

***Receipt of complaint by Customer Call Centre***

4.1. As per ASIC's standard procedure, when it received the call making the privacy complaint on 27 October 2017, the caller was directed to ASIC's privacy webpage, with instructions to notify his concerns via the webpage (which would have directed the complainant to the feedback@asic.gov.au email address).

4.2. Since the privacy breach, the CCC has introduced a new practice, known as *#hotissue*. This is described as any contact or enquiry raised by a customer or an observation made by a Registry team member, which may require urgent attention and response from ASIC. Staff across the CCC have been trained to raise a potential breach by ASIC of an APP as a #hotissue with the Helpdesk or their supervisor immediately, and to log the concern in a central Registry register as a #hotissue. Concerns are then to be escalated to a senior manager, Registry legal or CLO or the Registry Manager as required.

4.3. We consider the #hotissue practice to be an appropriate mechanism for ensuring staff act promptly on privacy concerns. We recommend that similar practices be put on place for all ASIC staff to ensure that all ASIC staff are trained on the importance of immediately passing on any privacy concerns to a senior manager who can then escalate as required.

| **Recommendation 7 – ASIC train staff to immediately raise privacy concerns** | |
|---|---|
| ASIC train staff to implement an organisation wide practice to immediately raise any privacy concerns with a supervisor, so that they may be escalated as required. | |
| **ASIC Response:** | Agreed. |

4.4. We suggest that ASIC undertake regular checks to ensure that links to privacy pages on the ASIC website are functioning, so that ASIC customers are not discouraged from raising issues or complaints. APP 1 requires the agency to maintain a privacy policy which is up-to-date. Where an agency uses a layered privacy policy, as ASIC does, we think that could extend to ensuring links between the layers are operational.

| **Recommendation 8 – ASIC undertake regular checks of privacy links** | |
|---|---|
| ASIC undertake regular checks of privacy links. | |
| **ASIC Response:** | Agreed. |

## Process review – Complaint Management Policy

***Making of privacy complaints***

4.5. Since the privacy breach, ASIC has reviewed its complaints framework, and now all complaints are handled through the CAA framework. Information about ASIC's handling of privacy complaints through this framework is available in the CAA section of the website.[2] We recommend that a link to this information be added to the ASIC Privacy Policy, in addition to the existing link enabling customers to submit a complaint online.[3]

| **Recommendation 9 – ASIC add a link to CAA privacy page to its privacy policy** | |
|---|---|
| ASIC add a link to the webpage titled 'complaints about our handling of your privacy' in the CAA section of its website to its privacy policy. | |
| **ASIC Response:** | Agreed. |

4.6. To ensure no complaint is overlooked, when concerns are raised, ASIC should ensure staff are trained to clarify with the individual if they wish to make a complaint (if required), and if desirable from an internal process perspective, feed the complaint into the system on the individual's behalf.

4.7. It should also be made clear that even where the individual does not wish to make a complaint, the concerns should still be raised with a supervisor to determine whether the matter should be escalated.

| **Recommendation 10 – ASIC train staff to lodge privacy complaints** | |
|---|---|
| ASIC train staff to ensure complaints made other than via the CAA are nonetheless appropriately progressed internally, and where there is doubt to clarify with an individual raising concerns whether they wish to lodge a privacy complaint. | |
| **ASIC Response:** | Agreed. |

***Logging and classification of the complaint***

4.8. Upon the issue being brought to her attention on 30 October 2017, the CLO Complaints Officer efficiently reviewed the complainant's previous contact with ASIC and determined to log a complaint.

4.9. In triaging the complaint, the CLO Complaints Officer identified that the complaint raised concerns about a potential breach of the APPs, as well as concerns about a Registry product. However, instead of directing the privacy complaint to Commission

[2] http://www.asic.gov.au/about-asic/contact-us/how-can-we-help-you/complaints-about-asic/complaints-about-our-handling-of-your-privacy/

[3] http://www.asic.gov.au/about-asic/dealing-with-asic/privacy/asic-privacy-policy/asic-privacy-policy-our-personal-information-handling-practices/#complaints

Counsel as specified in the Complaints Management Policy, it was directed to Registry to undertake an assessment of the complaint.

4.10. Given that it may be difficult for the CLO Complaints Officer to quickly determine whether a privacy issue has been raised, we recommend that all CAA raising 'privacy' as an issue or concern should be either (a) allocated directly to Commission Counsel (who can then re-allocate as necessary); or (b) information about each complaint is provided to Commission Counsel at the same time as sending the complaint to a different team. Under either option, privacy concerns will be quickly assessed by members of the privacy team with specialist knowledge of the *Privacy Act 1988*.

| **Recommendation 11 – All privacy CAA be referred to CLO for assessment** | |
|---|---|
| ASIC ensure that all complaints raising privacy issues or concerns be brought to the attention of the privacy team within the CLO for assessment on whether CLO should be involved. | |
| **ASIC Response:** | Agreed. |

4.11. ASIC should also ensure that the CLO Complaints Officer has sufficient training to identify privacy issues in complaints which may not expressly raise privacy concerns, so that these matters can be similarly referred to the privacy team for assessment.

| **Recommendation 12 – CLO Complaints Officer training** | |
|---|---|
| ASIC implement specific training for CLO Complaints Officers on identification of potential privacy issues in complaints, and the process for referring issues for assessment by the privacy team. | |
| **ASIC Response:** | Agreed. |

4.12. We note that since the privacy breach, ASIC have introduced a system where an email is sent to a dedicated privacy email address every time a CAA raises privacy concerns or issues. Subject to regular monitoring and efficient triaging of the inbox, we consider this to be an appropriate response to Recommendation 11.

***Risk assessment of privacy complaints***

4.13. In the case of the 27 October 2017 complaint, both the Complaints Officer and the Registry Legal Officer told AGS that they undertook a preliminary review of the complaint upon receipt. However, as it was not identified at that time that the complaint concerned personal information, it was not appreciated that a privacy breach had occurred, or that there was a potential for ongoing breaches.

4.14. Given that legal officers within business areas are likely to have general but not specialist knowledge of privacy, in the case of future privacy complaints, we recommend that a preliminary risk assessment be undertaken as soon as possible after receipt by a member, or in conjunction with a member, of the privacy team. ASIC should ensure that lawyers undertaking such assessments have appropriate training and knowledge to ensure that issues can be quickly identified and actioned.

| **Recommendation 13 – CLO undertake prelim assessment of privacy complaints** | |
|---|---|
| A preliminary risk assessment of any complaint raising privacy issues be undertaken by, or in conjunction with, a member of the privacy team. | |
| **ASIC Response:** | Agreed. |

| **Recommendation 14 – Privacy team training regarding handling privacy complaints** | |
|---|---|
| ASIC train privacy team staff to handle privacy complaints, including undertaking preliminary assessments. ASIC ensure that lawyers undertaking such assessments have appropriate knowledge of privacy issues, as well as ASIC policies and procedures. | |
| **ASIC Response:** | Agreed. |

4.15. Where a privacy breach is suspected or identified, ASIC should seek to activate a data breach response plan detailing appropriate measures to contain and evaluate the breach, notify affected individuals and prevent further breaches. The Complaints guidance should clearly provide that ASIC will respond to suspected or actual privacy breaches in accordance with its data breach response plan.

4.16. We note that subsequent to the privacy breach, ASIC has taken steps to accelerate the development of its data breach response plan.[4] We recommend that as part of that plan, ASIC appoint a data breach response team responsible for responding to personal information breaches.

| **Recommendation 15 – Implementation of a data breach response plan** |
|---|
| (d) ASIC finalise and implement a data breach response plan, including the appointment of a data breach response team. |
| (e) ASIC train the data breach response team to implement the data breach response plan. |

[4] A Cyber Security Incident Management Plan was already in place.

| | |
|---|---|
| (f) ASIC update its Complaints Guidance to reflect that ASIC will respond to suspected or actual privacy breaches in accordance with its data breach response plan. | |
| **ASIC Response:** | Agreed. This recommendation is already in progress. |

**Process review - staff education and training**

4.17. From our discussions with individual officers, we understand that all ASIC staff are required to undertake privacy training as part of their induction program. Staff must then complete an online training module annually regarding the APPs.

4.18. Additionally, ASIC has recently completed an organisation-wide review of the personal information it handles. As part of this review, ASIC has:

4.18.1. conducted an agency wide survey checking compliance with the APPs;

4.18.2. analysed the survey responses to identify gaps in ASIC's compliance and where additional training is required;

4.18.3. updated its Privacy Policy;

4.18.4. provided guidance on conducting privacy impact assessments; and

4.18.5. engaged AGS to draft a privacy manual to guide staff on privacy issues including how to deal with a privacy inquiry or alleged breach, good privacy practices, collection of personal information and collection notices.

4.19. We recommend that this manual, as well as other resources such as issue-specific factsheets, be published on the privacy resource page on ASIC's intranet so that it may be accessed by staff at any time.

| **Recommendation 16 – Continued development of privacy resources** | |
|---|---|
| ASIC develop privacy resources, including a manual to guide handling of personal information, to be published on the privacy resource page on its intranet. | |
| **ASIC Response:** | Agreed. Already in progress. |

4.20. Additionally, we note that from 1 July 2018, s 16 of the Privacy Code will require an agency to:

4.20.1. include appropriate privacy education or training in any staff induction program it provides. The privacy education must address the privacy obligations of agency staff, and agency policies and procedures relating to privacy

4.20.2. take reasonable steps to provide appropriate privacy education or training annually to all staff who have access to personal information in the course of performing their duties as a staff member.

4.21. Given the matters raised above, we recommend that ASIC update its induction program to ensure that staff are trained to identify and report privacy concerns, have knowledge of the data breach response plan and can readily locate key resources to guide their response to privacy issues. Similarly, ASIC should ensure that these matters are covered in annual training for staff.

| **Recommendation 17 – ASIC update induction and annual staff training** | |
|---|---|
| ASIC review its induction and annual privacy training to ensure that staff are trained to effectively identify and report privacy concerns, have knowledge of the data breach response plan and can locate key privacy resources. | |
| **ASIC Response:** | Agreed. |

4.22. We also recommend that ASIC seek to increase the knowledge of all of its legal officers to ensure that potential privacy issues are expediently identified and referred to the privacy team for preliminary assessment and triage. Such training should be in addition to the mandated legal training, include detailed consideration of the definition of personal information as well as the implementation of the data breach response plan.

| **Recommendation 18 – Legal officer training** | |
|---|---|
| ASIC implement specific training for legal officers outside CLO, or at a minimum, the privacy champion for each non-CLO legal team, on identification of potential privacy issues, the process for referring issues for assessment by the privacy team, and the implementation of the data breach response plan. | |
| **ASIC Response:** | Agreed. |

### Other matters – handling of 28 August 2017 complaint

4.23. As set out in the chronology below, there was also an earlier call received to the CCC on 28 August 2017 raising the privacy issue with the Service, but this was not progressed by the CSO.

4.24. ASIC have flagged their intention to create a further module specific to CSO staff addressing how the APPs apply to their work to commence in the first quarter of 2018 in the following terms:

> This will be a classroom facilitated session presented by a trainer. Supporting materials including a video introduction into the Australian Privacy Principles and module content specific to the line of work the staff member will be completing. The training session will

be concluded with an assessment activity which must be completed to a satisfactory level prior to commencing work. e.g. prior to taking telephone enquiries.

4.25. Additionally, ASIC are currently investigating options for skills validation and competency assessment upon completion of induction training. This testing will be used to ensure that a CSO is able to undertake the work after training before being placed to receive calls.

4.26. Furthermore, ASIC advise that since August 2017, changes have been made to staff training. Following staff induction, new trainees are currently co-located in the 'Learning Hub'. While in the Learning Hub, CSOs are provided with a higher level of support to consolidate learning before they join a CCC team.

4.27. In order to reduce the risk of similar instances occurring, we recommend that ASIC introduce further quality assurance (of the type proposed by ASIC). We further suggest ASIC ensure that it is reinforced with new CSOs that issues or concerns can be raised with not only a supervisor, but also floor walkers, performance coaches and/or the helpdesk where a supervisor is unavailable.

| **Recommendation 19 – CCC staff training, quality assurance and supervision** | |
|---|---|
| (d) ASIC continue to deliver tailored training to CCC staff.<br>(e) ASIC undertake quality assurance assessment to ensure that call centre staff are able to receive calls and adequately address issues before commencing work.<br>(f) ASIC ensure CSOs are trained to raise concerns with other staff, including their supervisor, floor walkers, performance coaches and the helpdesk, where their supervisor is unavailable. | |
| **ASIC Response:** | Agreed. |

## 5. PART 3 – RESPONSE TO DATA BREACH

### Implementation review – Response to data breach

***Step 1: contain the breach***

5.1. Late in the day on 8 November 2017, senior managers in Registry and IT were made aware that there had been a media enquiry about the privacy issue with the Service. Further to discussions with IT management, the Senior Executive Leader of Registry decided that the Service should remain active until an assessment of the issue could be undertaken. The COO of ASIC instructed that the service be disabled at 5.30am the following day.

5.2. From our discussions, it is apparent that the response of management to not disable the Service on 27 October 2017 was because, ASIC had not at that time identified the privacy breach. We acknowledge the customer-service motivations behind management's reluctance to disable the Service without a full investigation. The failure to identify and process the issue as an actual or potential privacy beach meant that management were not sufficiently informed to respond immediately and appropriately.

| **Recommendation 20 – ASIC take immediate steps to contain potential breaches** | |
|---|---|
| The ASIC data breach response plan provide that immediate steps should be taken to contain any actual or suspected privacy breach (regardless of whether a full assessment of the suspected breach has been carried out). | |
| **ASIC Response:** | Agreed. Already in progress. |

5.3. After a decision was made around 5:30am on 9 November 2017 to take down the service, steps were taken within approximately 4 hours to remove the service from ASIC's website and check that the function could no longer be accessed. In our view, the functionality was quickly disabled after a decision was taken for this to occur.

5.4. Consistent with our recommendation above, we suggest that ASIC undertake a PIA before the service recommences operation to ensure not only compliance with the Privacy Act, but that any privacy impacts from the service are limited as much as possible.

| **Recommendation 21 – ASIC undertake PIA before Service recommences** | |
|---|---|
| ASIC undertake a PIA on the Service, as amended, before it recommences operation. | |
| **ASIC Response:** | Agreed. |

***Preliminary assessment***

5.5. After the decision to disable the service was made, ASIC acted swiftly to internally escalate the complaint. Senior Registry, IT and CLO staff formed a de-facto data breach response team, and contributed to ASIC's response to the privacy breach. The complaint was treated seriously and considered steps informed by legal advice were taken to respond to the breach.

5.6. On the same day as the service was disabled, in accordance with the guidance set out in the OAIC Data Breach Notification Guide, ASIC undertook an initial assessment and evaluation of the risks of the breach.

5.7. In summary, ASIC concluded if a data breach had occurred there was a potential for harm. Based on this assessment ASIC immediately commenced an investigation to:

5.7.1. identify any individuals whose privacy may have been breached; and

5.7.2. notify those individuals that may have suffered serious harm.

5.8. ASIC engaged Deloittes to assist in identifying individuals who should be notified about the potential breach of personal information.

5.9. As set out in the chronology below, ASIC issued a public statement notifying the public of the breach on 15 November 2017. On the same date, ASIC provided written notification to the OAIC of the data breach.

***Step 2: evaluate the risks associated with the breach***

*Individuals affected by the breach*

5.10. Subsequent to ASIC's detailed preliminary assessment, ASIC engaged Deloitte to review the audit logs kept for the service and identify individuals potentially affected by the breach.

5.11. At the outset, it was identified that audit logs of searches conducted using the function were only kept for a period of 90 days (before 1 July 2017). This limited ASIC's ability to identify individuals that may have been affected by a privacy breach before 1 July 2017, or affected by a privacy breach after that date because another individual, without authorisation, accessed their personal information.

5.12. To overcome this issue, IT should ensure that appropriate audit logs are created to capture records of how all personal information is handled by a system. This should be built into any system development or upgrade, and may require a review of existing services to ensure that adequate logging occurs.

| **Recommendation 22 – All handling of personal information to be recorded in logs** | |
|---|---|
| ASIC develop a risk based approach to ensure where appropriate the handling of all personal information by new and existing systems be recorded in an audit log. | |
| **ASIC Response:** | Agreed. |

5.13. Subsequent to the breach, ASIC have also extended the storage period of audit logs for the service from 94 days to 400 days. While AGS is unaware of any industry standard for the retention of audit logs, we consider the proposed period of time to be adequate. We suggest that ASIC review the audit log retention period for all other services and systems and ensure that the retention period for those services is adequate based on the nature of the service, types of personal information handled and potential risk of harm if misuse occurs.

| **Recommendation 23 – ASIC review the storage period of all audit logs** | |
|---|---|
| ASIC review the storage period of all audit logs and ensure retention periods are adequate based on the nature of the service, types of information handled and the potential risk of harm if misuse occurs. | |
| **ASIC Response:** | Agreed. Since 2016 all new systems have been built in compliance with the Record retention requirements under the National Archives Act. |

5.14. Deloitte concluded that there were 770 identifiable affected customers whose purchased products were either viewed or forwarded onto a different email address than the one attached to the search data. We note that across November 2017, ASIC took steps to notify those affected customers which we discuss further below.

*Extent of the breach*

5.15. Even where a search did not return a result ie no search history (nil result) and no email address was logged, we consider that a potential privacy breach occurred as information disclosed in response to the search constitutes personal information.[5] Although this information does not at face value appear to be sensitive information, and the risk of harm from a 'nil result' search may be considerably lesser than where a result is returned, a nil result still says something about a person if they are identifiable from their email address.[6] Specifically, that they have not used their email address to undertake a paid search in ASIC's registers in the past 90 days.

5.16. For these reasons, we consider that the number of potential privacy breaches which may have occurred through use of the search is much higher. Given our view that only searches which lead to a purchase being sent to the same email address or an ASIC address should be presumed to be authorised,[7] we consider as many as 6,131[8] privacy breaches may have occurred through use of the Service.

---

5 A 'nil result' may be returned in a number of circumstances. These are discussed below in more detail at paragraph 5.28.

6 Conceivably, harm could also flow from a 'no result'. For example, the absence of any purchases may, in itself, be valuable information to a business competitor.

7 Presumably, as access to the information was required or authorised by law.

8 6,760 total searches minus 629 searches sent to the same email or an ASIC email address.

5.17. While AGS acknowledges that there are a number of reasons why a 'nil result' might be returned, these figures do suggest that there is a risk of phishing by individuals using the service. ASIC undertook statistical analysis of the 'nil result' searches which showed they were spread fairly evenly across the period, averaging around 25 a day. This indicates that any instances of phishing are more likely to have been isolated individuals rather than coordinated enterprise-level attacks.

5.18. It is important that any reboot of the Service build in safeguards to enable the identification and prevention of phishing activity. We recommend IT give particular thought to how systems can be used to detect and respond to any suspected phishing through the Service.

| **Recommendation 24 – ASIC review risk and guard against phishing** | |
|---|---|
| ASIC ensure that in any reboot of the Service, IT consider implementing systems solutions that enable ASIC to detect and respond to any suspected phishing through the Service. | |
| **ASIC Response:** | Agreed. |

*Assessment of harm*

5.19. Based on its investigation, ASIC completed a preliminary assessment of harm. [9]

5.20. To encourage privacy compliance, we suggest that future privacy training cover not just the legislative requirements in the APPs, but also the consequences of failing to comply with those responsibilities (both for individuals and the agency).

| **Recommendation 25 – ASIC privacy training cover potential harm from breaches** | |
|---|---|
| ASIC privacy training cover the potential consequences of a privacy breach, including potential harm to individuals and to the agency. | |
| **ASIC Response:** | Agreed. |

***Step 3: notification to potentially affected third parties***

5.21. Having assessed that a real risk of serious harm could flow to an individual if search results were viewed, ASIC appropriately determined to:

5.21.1. notify the OAIC on 15 November 2017 of the privacy breach

5.21.2. publish a public notification of the privacy breach on its website on 15 November 2017

5.21.3. provide formal, written notification to the OAIC on 15 November 2017 of the privacy breach, as well as an update on relevant matters

9 Attached to the OAIC notification dated 15 November 2017.

5.21.4. between 24 November 2017 and 27 November 2017, send a total of 770 individualised emails to customers it had identified as potentially affected by the breach.

5.22. So that ASIC is positioned to respond to any future eligible data breaches in accordance with the amendments to commence on 18 February 2018, we recommend that ASIC's privacy team undertake training as to the contents of the notifiable data breaches scheme.

| **Recommendation 26 – Privacy team training re Notifiable Data Breach scheme** | |
|---|---|
| ASIC ensure privacy team staff receiving training regarding the Notifiable Data Breaches scheme | |
| **ASIC Response:** | Agreed. |

*Publication of notice on ASIC's website*

5.23. A notice about the privacy breach was published on ASIC Connect on 15 November 2017. AGS recommends that as part of training received by the privacy team on the new notifiable data breach scheme, staff are trained on the preparation of data breach notices with reference to lessons learned from this incident (see Recommendation 27 below).

*Emails to customers*

5.24. We are advised that 770 individual emails were sent out notifying affected customers of the potential breach. As above, based on the Deloitte data, these were sent to two categories of affected customers: customers whose email address had been used to view previous histories and people whose previous search history had been sent to a different email address.

5.25. We recommend that privacy team training on the Notifiable Data Breach scheme incorporate learnings from this incident, particularly around balancing the need to provide fulsome information, with the need for immediacy, and the need to consider the privacy of other individuals where relevant.

| **Recommendation 27 – Privacy team training on preparation of data breach notices** | |
|---|---|
| ASIC ensure that privacy team staff are trained on the preparation of data breach notices with reference to lessons learned from this incident. | |
| **ASIC Response:** | Agreed. |

*Actual harm*

5.26. To date, ASIC has only been advised of one other actual breach of privacy other than the matters raised in the Guardian article. In that regard, we note that in all of

the responses received to individual notification emails, there were no reports of actual harm. Many of the responses, while concerned about the potential breach, were positive about ASIC's steps to notify of the risk.

5.27. Conclusions about the extent, scope or seriousness of the breach should be qualified given harm cannot be easily quantified. ASIC itself has treated the breach seriously, and in accepting recommendations made in this report, committed to improve policies, procedures and training which will lead to positive advancements in the manner in which personal information is protected by the agency.

***Step 4: prevent future breaches***

5.28. In our discussions with ASIC, it is clear that steps are already being taken to implement measures to prevent future privacy breaches, including:

5.28.1. the audit log retention period for paid searches has been extended to 400 days

5.28.2. the #hotissues policy has been implemented

5.28.3. a new privacy specific email address has been created for referral of privacy issues and complaints.

5.29. Additionally, by engaging AGS to review the events leading up to, and ASIC's response to the breach, this report has identified a large number of opportunities for ASIC to improve its policies, practices and procedures. Critically, AGS has been engaged to prepare a data breach response plan and deliver training to key staff on that plan's implementation.

| **Recommendation 28 – ASIC consider review of Registry system upgrades** | |
|---|---|
| ASIC should undertake a risk-based assessment of Registry system upgrades involving handling personal information where no assessment of potential privacy impacts was undertaken. | |
| **ASIC Response:** | Agreed. |

## 6. SUMMARY CHRONOLOGY

| Date | Description |
|---|---|
| **Aug-Oct 2016** | The search history function was developed. On 21 October 2016, final approval for the service was given by the Senior Executive Leader of Registry. |
| **Jan-Apr 2017** | System and Usual Accepting Testing was undertaken to ensure that all Service functionalities worked as expected. |
| **13.05.17** | ASIC launched the search retrieval service. |
| **28.08.17** | The Customer Complaints Centre (**CCC**) received the first complaint about the search history function. The complaint was not escalated. |
| **27.10.17** | The CCC received the second complaint about the search history function. At the recommendation of the CCC, the complainant, in an effort to report the complaint, emailed feedback@asic.gov.au to advise of an issue with the privacy complaint link. |
| **30.10.17** | IT fixed the issue with the privacy complaint link and advised the complainant. The complainant sought an update about his complaint. The complaint was forwarded to CLO, who register the complaint in the database and allocate it to Registry |
| **31.10.17** | Registry acknowledge receipt of the complaint with the complainant. Registry Legal and SOS are consulted, but are not able to respond immediately. |
| **03.11.17** | The complainant sought a further update from Registry. Registry Legal agreed to review the complaint and the complainant was advised of the same. |
| **08.11.17** | The complainant sought a further update and states he would advise the media and the 'privacy ombudsman' if no response was received. The Media Unit subsequently received an enquiry from a journalist and advised senior management in IT and Registry. |
| **09.11.17** | The Guardian article was published.<br>The search history function was disabled. ASIC commenced an investigation as to the nature, extent and likelihood of any personal information breach. |
| **10.11.17** | ASIC undertook an analysis of the access and use data with Deloittes. |
| **15.11.17** | ASIC notified the OAIC in writing of a potential data breach and publish a statement on its website. |
| **24.11.17 – 01.12.17** | ASIC sends individualised emails to customers whose personal information may have been the subject of unauthorised disclosure. ASIC receives 26 responses overall. |