CUSTOMER OWNED BANKING
CODE COMPLIANCE COMMITTEE

Compliance with privacy obligations follow-up inquiry outcomes

Follow-up inquiry into how Code subscribers applied recommendations issued by the Customer Owned Banking Code Compliance Committee to improve compliance with privacy obligations under Section D23 and Key Promise 8 of the Customer Owned Banking Code of Practice.

June 2020

Contents

Executive summary

Background

Part D Section 23 of the Customer Owned Banking Code of Practice (the Code) details commitments relating to information privacy and security that Code subscribers will uphold.

In 2018, the Customer Owned Banking Code Compliance Committee (the Committee) conducted an Own Motion Inquiry (OMI) into subscribers' compliance with this section of the Code. There was concern at the time about the high level of non-compliance among subscribers with privacy obligations in the Code.

Since the OMI, subsequent Annual Compliance Statements have indicated a rising number of self-reported breaches relating to privacy. This, together with recent government recommendations to update and strengthen privacy laws, prompted the Committee to conduct a further inquiry to determine whether Code subscribers have improved the way they manage their privacy and data security.

The further inquiry

The Committee aimed to find out whether Code subscribers had made use of the privacy compliance checklist and implemented the recommendations outlined in the 2018 Own Motion Inquiry into privacy.

To do this, the Committee gathered information from 62 Code-subscribing institutions with an online questionnaire (see Appendix 3) included as part of the 2019 Annual Compliance Statement (ACS) program.

In addition, telephone conferences were held with a selection of 20 Code subscribers to obtain specific details about privacy breaches, training, procedures, processing, reporting and clarification of privacy responses.

Conclusion

The Committee found that while Code subscribers told us they are committed to meeting their obligations, the recommendations and privacy checklist provided in the 2018 OMI have not been fully implemented by all Code subscribers. Processes and procedures are in place, but ongoing monitoring, review of processes and ensuring that staff are effectively trained need continued focus. Privacy and data security policies should be proactively maintained and reviewed at least annually, and many subscribers would benefit from formally documenting processes in key areas of their business that may have an increased risk of privacy breaches.

Overview of findings

Regular review of privacy policy

Privacy and data security

All Code subscribers told us they had conducted a review of these policies within the last 18 months, which speaks to their commitment to meeting their obligations. Most Code subscribers used a variety of sources to guide their policy changes. These included:

- Internal review outcomes
- Office of the Australian Information Commissioner (OAIC), Australian Financial Complaints Authority (AFCA) and GRC Solutions recommendations, and
- Australian Prudential and Regulation Authority (APRA) Prudential Standard CPS 234.

Regularly reviewing and updating privacy and data security policies is the most important way Code subscribers can continue to meet their obligations under the Code and in line with applicable legislation. Code subscribers should be proactive in maintaining privacy and data security policies, including conducting a review at least annually, ensuring availability of policies and embedding changes into their organisation's risk framework in a timely manner.

Key areas for consideration

Privacy policy

All Code subscribers say they ensure their privacy policy is accessible for customers and potential customers on their website and in other forms of communication. There is also consistency across Code subscribers regarding privacy notices during customer application processes. These are provided to customers at the time of application, whether it is via an online process or in person.

Some subscribers may use third parties who are located overseas. The majority of Code subscribers address overseas disclosures[1] in their privacy policies. Those that do not include these disclosures advised they do not use third parties for these purposes.

Obtaining oral privacy consent may be required when speaking with new customers, and subscribers were asked whether they considered using a script or pre-recorded message for this purpose. Almost half of Code subscribers say they use both for obtaining privacy consent and the majority of subscribers provide at least one method of privacy consent when speaking with potential customers. Their methods are often dictated by the size of the organisation and whether their interactions with customers are primarily online or in person.

Code subscribers should ensure that methods of communication in recording consents/authorities and notifications are well embedded in business processes to mitigate the risk of privacy breaches.

Code subscribers should be able to demonstrate that personal information is managed in an open and transparent way.

[1] See Appendix 2 APP8

Access to data and information

There are several ways to manage information security. This review focused on staff access to information and documents, password management and physical location audits.

Almost all Code subscribers indicate that staff access levels are reviewed regularly and in line with their job descriptions. A similar number of subscribers say they meet password protocols and ensure staff use strong passwords and do not share them with others. Subscribers conduct regular reviews and training which is consistent with our recommendations in the 2018 OMI.

The majority of Code subscribers appear consistent in their reviews on physical access and say they conduct them at least once annually. However, it was concerning that 23% of subscribers have not incorporated an audit relating to physical access at all locations into their review framework.

Code subscribers must protect personal information through all stages of the information lifecycle. Audits on physical access controls and system access controls at all locations (especially where personal information is held) should be implemented across the board as these are key to mitigate risks of unauthorised access or disclosure of personal information, modification of personal information or loss of personal information.

Document storage and destruction

Code subscribers must ensure that document retention, destruction and archiving procedures and processes are implemented to demonstrate compliance with privacy obligations to take reasonable steps to destroy or de-identify personal information that is no longer required.

Code subscribers were asked to provide clarification around their retention practices for both soft and hard copy documents in their organisations. Processes and procedures to ensure information is destroyed and/or de-identified was of particular interest.

Most Code subscribers have processes or procedures in place, or currently under review. Reviewing and understanding destruction protocols for off-site storage and scanning is also a consideration in this area.

Overall, good industry practice is evident with archiving procedures and retention periods in place for hard copy and soft copy documents onsite and offsite.

Privacy and data breaches

All Code subscribers say they have clearly defined roles and responsibilities within their organisations, which means breaches are less likely to be overlooked. This was a recommendation from the 2018 OMI and included on the privacy compliance checklist.

Most Code subscribers also have clear escalation processes for breach reporting; examples of good practice adopted by some Code subscribers include visual guides, such as flow charts, to make this process easier for staff.

More than half of respondents advised they had increased staff awareness and provided ongoing refresher training and regular reviews. Some organisations advised their current processes were adequate and working effectively with minimal or no breaches to report.

The Notifiable Data Breach (NDB) scheme reinforces the accountability of organisations to protect personal information. It is critical that policies and procedures for data breach notification are implemented, compliance tested and reviewed regularly.

This inquiry also asked about the extent of subscribers' Data Breach Response Plans (DBRP), including their process for reporting to the OAIC and notifying individuals at serious risk of a data breach.

A large majority of Code subscribers have policy and response plans in place which are scaled to the nature of the breach. Some subscribers have indicated they are currently developing or reviewing their processes to improve compliance with CPS 234. The remaining subscribers are currently considering a review of their systems and reporting. Most subscribers' DBRP includes the process to report to the OAIC and member reporting protocols depending on the severity of the breach.

Code subscribers must have a clear understanding of the Data Breach Notification practices in their organisations. This can be achieved through comprehensive training in DBRP policies and procedures.

Training

Staff training

All Code subscribers have indicated they have implemented training, but not all include training on how to report breaches. Almost all subscribers utilise a mix of formal and informal training methods to effectively meet different learning styles. Subscribers are also in varying stages of including DBRP training. Some advised they have scheduled this training whereas others are still reviewing their current privacy training for integration.

All privacy training material should be reviewed to ensure that data breach notification training is included in all privacy training activity and that the training is consistently and regularly rolled out by all Code subscribers. An organisation's DBRP should be reviewed to ensure staff understand how to identify and report data breaches as well as take action to minimise potential breaches. It is important that training also includes learning checks to test staff knowledge.

Embed compliance into a risk framework

All Code subscribers must embed privacy compliance into their risk framework to demonstrate compliance.

Code subscribers were asked to consider ways they can embed compliance with privacy obligations into their company's risk framework. Respondents indicated they use a wide range of methods to incorporate privacy compliance, including: regular policy reviews; role plays in training; desktop flyers promoting privacy and information security; and staff training.

Almost all Code subscribers also conduct privacy reviews regularly and many are included as part of internal and external audit programs.

Review compliance

Code subscribers were asked about their organisation’s approach to reviewing compliance with data and security policies.

Clean desk policies: All Code subscribers have privacy safeguards in place and incorporate either official or unofficial desk sweeps. Identified breaches are then addressed with employees.

Shadow shopping calls: Staff phone monitoring (instead of shadow shopping calls) was noted in most Code subscriber responses, with quality assurance results reported to senior management and used for ongoing training.

Privacy notices on organisation website: All Code subscribers display their privacy notices and policies on their websites.

Tax file number (TFN) retention and access: All Code subscribers have TFN retention processes and restricted access, where required.

Provide an opt-out for customer direct marketing: All Code subscribers who use marketing material include an opt-out option. Some who send quarterly, or half-yearly newsletters do not have an opt-out option. Code subscribers who issue newsletters should review their processes and content to confirm whether the newsletter is direct marketing for which an opt-out option is required.

Providing information to guarantors: Almost all Code subscribers have a privacy consent policy or procedure for guarantors to have access to any information relevant to loan balances. All subscribers require guarantors to be identified before any information is provided.

Code subscribers must continue with the strategies that are being used to evaluate the appropriateness and effectiveness of privacy practices currently being used. To assist in the review of the effectiveness of processes, a four-step framework for privacy compliance is recommended in the detailed findings later in this report.

Protecting privacy in arrangements with third parties

Third party review

Code subscribers were asked questions about whether they had conducted due diligence on third-party data security arrangements and sought legal advice when preparing contracts to ensure privacy and data breach clauses are sufficient.

The majority of Code subscribers advise their contracts contain sufficient reporting clauses which have been developed in line with APRA’s CPS 234.

It is important to review new and existing third-party arrangements against privacy and data measures and agreed service levels. Most subscribers have contracts in place with relevant clauses relating to the use of personal information. These subscribers also monitor service level agreements (SLAs) and issue reports to executive staff on a monthly or quarterly basis.

Almost all Code subscribers conduct a privacy impact and risk assessment prior to engagement with third party providers. Code subscribers should review all contracts that involve the handling of personal information prior to execution or renewal, incorporate the use of checklists and ensure additional consideration is given to areas assessed as having a greater risk.

Privacy Impact Assessments are an effective management tool and should be undertaken for all projects or decisions that involve new or changed personal information handling practices, including implementing new technologies.

Introduction

The Customer Owned Banking Code Compliance Committee (the Committee) conducted an inquiry into Code subscriber’s compliance with privacy obligations following its 2018 own motion inquiry (OMI) into privacy dated 26 June 2018 (see Appendix 6).

Following publication of the recommendations, the Committee conducted a follow up inquiry into how Code subscribers comply with privacy obligations under Section D23 and Key Promise 8 of the Customer Owned Banking Code of Practice. A particular focus of this inquiry is the review process Code subscribers have undertaken since the 2018 OMI and the actions taken in response to the recommendations and checklist issued by the Committee.

This report describes the findings of the follow-up inquiry and good practice that Code subscribers should follow.

Privacy

Privacy and data security are crucial areas of compliance for customer owned banking institutions, and the importance and complexity of these obligations is increasing. The Code requires subscribers to comply with the Privacy Act 1988 and the Australian Privacy Principles (APP).

About the inquiry

Inquiry objectives

The objective of this inquiry was to follow up with Code subscribers to determine whether they had implemented the recommendations and used the checklist outlined in the 2018 OMI.

Inquiry methodology

This inquiry was based on information provided by Code subscribers and the Committee’s analysis of that information. Information was gathered via the Annual Compliance Statement (ACS) in the form of a questionnaire. An online questionnaire was sent to all Code subscribers (see Appendix 3).

Additional information was also obtained via telephone conferences with 20 Code subscribers. The telephone conferences were undertaken as part of the 2019 ACS verification program to obtain specific details about privacy breaches, training, procedures, processing, reporting and clarification of privacy responses.

The previous OMI considered the privacy procedures in place at each subscriber and how compliance with privacy obligations is managed. Recommendations on how to improve and maintain compliance with the Privacy Act and the Code were then developed to guide Code subscribers.

Participating institutions are categorised by size, measured by assets and number of active members (see Appendix 5).

Review of privacy policy

All institutions benefit from consistently and comprehensively reviewing their privacy and data security policies. Code subscribers should implement procedural change when issues are identified and work to embed these in the organisation’s risk framework.

Privacy and data security[2]

Almost all Code subscribers (95%) told us they undertook a review of their privacy and data security policy and practices in the 12 months prior to the ACS. In some instances, external lawyers were used for this review. Two smaller Code subscribers indicated they had not undertaken a review, but one was scheduled for later in 2019.

Generally, Code subscribers review and update their policies annually or when legislative changes have been introduced (e.g. AFCA updates, GRC recommendations and guidance from the Office of the Australian Information Commissioner (OAIC)). After the most recent review, 83% of Code subscribers updated their policies and procedures. Data security policies were also updated to reflect APRA Prudential Standard CPS 234 Information Security. Those subscribers who did not make changes advised that a review is scheduled in the near future.

Five Code subscribers (8%) advised their procedures had been reviewed just prior to the June 2018 OMI report and they did not have another review scheduled at the time. Some Code subscribers reviewed their procedures at a later stage or as part of their annual review process rather than as an individual privacy review process. Other Code subscribers indicated they had completed an internal review on their Information Security Policy and Tool Framework in early 2019 or it is due later in 2019. Reviews included an update of existing policies and gaps. Some Code subscribers advised their privacy and data security policies had been reviewed internally, and they had received external advice and guidance in the last 12 months.

Findings:

The high number of Code subscribers who reported reviewing their privacy and data policies within 12 months is a pleasing result and shows the willingness of Code subscribers to regularly consider the veracity of their policy and practices.

To follow good practice Code subscribers should be proactive in maintaining privacy and data security policies, including conducting a review at least annually, ensuring availability of policies and embedding changes into their organisation's risk framework in a timely manner.

[2] See Appendix 3, questions 6.1.1 to 6.1.2

Key areas for consideration

There are a number of key focus areas that Code subscribers need to consider ensuring privacy obligations are met within their organisation.

Privacy policy[3]

It is important that privacy policies are easily available to customers and potential customers. All Code subscribers advised that their own privacy policies were easily accessible, whether on their websites, in branches or by mail upon request.

When reviewing privacy notifications on customer application processes, there is consistency across all Code subscribers. Generally, privacy notifications are provided to customers at the time of application, whether that is online or in person. Most Code subscribers (87%) allow customers to apply both online and in person. Some Code subscribers do not have an online application facility, so the privacy policy is always provided as a hard copy. Some Code subscribers provide their privacy notification as part of a welcome pack.

Scripts or pre-recorded messages are recommended to obtain privacy consent from potential customers. The majority of Code subscribers provide at least one method when speaking with customers. Just under half of Code subscribers (45%) have a script for oral consent as well as a pre-recorded message. Some Code subscribers are not considering the use of scripts or pre-recorded messages because they do not consider it necessary due to the size of their organisations. These subscribers usually have more face-to-face discussions with potential customers.

Other subscriber responses include a variety of methods to obtain privacy consent such as a verbal consent used by staff when accessing credit information during credit applications, call-recording disclosures for calls to and from contact centres and standard oral consent on loan processes. Some subscribers also refer customers to their website for the privacy notice.

A subscriber's privacy policy should also address how an organisation deals with overseas disclosures. Most Code subscribers (87%) say they have policies that address this and ensure the policy is provided when overseas disclosure is likely. Code subscribers whose privacy policy does not address overseas disclosures have advised they do not disclose information to overseas recipients. Many of these Code subscribers do not operate or deal with third parties that operate overseas.

Findings:

Code subscribers should be able to demonstrate that personal information is managed in an open and transparent way.

All Code subscribers reported that their privacy policies are readily accessible to existing and potential customers.

Code subscribers should ensure that methods of communication in recording

[3] See Appendix 3, questions 6.2.1 to 6.2.4

consents/authorities and notifications are well embedded in business processes to mitigate risk of privacy breaches.

To follow good practice such policies should be available on the website and the customer's chosen method of communication, if requested. Privacy consents and notifications should be provided via several communication methods depending on the organisation's size and application processes. This should be reviewed and updated as application processes change; e.g. incorporate online privacy notifications if online customer applications become available.

It is important that Code subscribers continue to regularly and proactively review and update privacy policies to ensure that any changes to the business and its processes are captured. This is especially important when addressing overseas disclosures.

Access to data and information[4]

Maintaining correct staff access levels to the banking system and internal documents is key to maintaining privacy protocols. There are several ways to manage information security. This review focuses on staff access to information and documents, password management and physical location audits.

Code subscribers should conduct an annual review and ensure staff access levels are up-to-date and consistent with all job descriptions. The majority of subscribers (97%) advised they are compliant with this recommendation. The remaining two subscribers are currently reviewing their processes.

Password management is another way to maintain privacy protocols. Passwords should be strong and never shared. Almost all Code subscribers require their staff to change passwords regularly and offer regular reviews and training in this matter. Several Code subscribers review password protocols quarterly or annually. Generally, subscriber behaviours regarding password management adhere to protocol and include regular review.

Most Code subscribers (77%) show consistency in regularly reviewing physical access at their locations. This includes some Code subscribers making a monthly attestation in their risk management records. In some cases, senior staff have visited sites to conduct random checks and carry out an audit on security access codes when there has been a change of staff. In some locations, access is controlled by electronic passes and access to branch keys and alarm codes is strictly monitored. They advise that access passes are reviewed quarterly to ensure they are issued to authorised staff only. Some Code subscribers who do not perform formal audits had small or single branch operations.

Findings:

Staff access to data and information is an important consideration for Code subscribers and the Committee is pleased with the dedication to compliance in this matter. To follow good practice Code subscribers should review staff access levels to the banking system and internal documents at least annually to ensure consistency with job descriptions.

[4] See Appendix 3, questions 6.2.5 to 6.2.7

Overall, good industry practice is evident with archiving procedures and retention periods in place for hard copy and soft copy documents onsite and offsite. The Committee however notes that 23% of Code subscribers have not incorporated an audit on physical access at all locations. This is concerning as it presents a risk for a privacy or data breach to be missed. This was previously recommended in the 2018 OMI checklist.

Audits on physical access controls and system access controls at all locations (especially where personal information is held) should be implemented as these are key to mitigate risks of unauthorised access or disclosure of personal information, modification of personal information or loss of personal information. Code subscribers should ensure they have sound processes relating to physical access at organisation locations. It should be part of annual audits and included as part of their privacy compliance checklists.

Document storage and destruction[5]

Processes for retaining documents and having appropriate destruction or de-identifying methods when they are no longer required is critical to meeting privacy requirements. There was a strong positive response to this question by Code subscribers with 92% indicating they have processes and procedures in place. Others have their policy under review. Some Code subscribers use the Customer Owned Banking Association's (COBA) retention guide as a model. Responses to this question include subscribers having destruction programs for obsolete soft copy records, and secure destruction bins for physical documents. Some subscribers also keep a record retention schedule within an associated policy.

It is common for this industry to use off-site storage and scanning facilities and many Code subscribers have indicated they have processes in place for reviewing these facilities. These processes are governed by various archiving procedures including the destruction of offsite documents after seven years. Only two Code subscribers do not have processes relating to off-site storage and scanning as they do not use these facilities.

Findings:

Overall there is good industry practice with this measure and Code subscribers have archiving procedures and retention periods in place.

To follow good practice Code subscribers should maintain organisation-wide initiatives to enhance compliance in relation to destruction or de-identification of information that is no longer needed. Retention schedules should also be reviewed to include soft copy data.

Code subscribers should review and update their document archiving and destruction procedures periodically to ensure compliant protocols are in place to meet privacy standards.

Code subscribers must ensure that document retention, destruction and archiving procedures and processes are implemented to demonstrate compliance with privacy obligations to take reasonable steps to destroy or de-identify personal information that is no longer required.

[5] See Appendix 3, questions 6.2.8 to 6.2.9

Privacy and data breaches[6]

Most subscribers focus on staff awareness and training to prevent privacy breaches and are confident their processes are adequate. More than half of Code subscribers do this by offering ongoing refresher training and register reviews. Training relating to privacy policies is provided to staff on an annual basis and further training is provided if there is a suspected breach.

Some subscribers indicated that post incident reviews are conducted on more significant events to assess remediation effectiveness. Subscribers who indicated they are not conducting reviews of their register advise there are minimal privacy breaches occurring and their internal controls and processes are working effectively. A small number of respondents identified a breach as human error and conducted appropriate training to rectify the issue. One Code subscriber identified only one privacy breach in seven years. After an internal review, the subscriber then reviewed their third-party processes and controls to determine that the incident was isolated. For some subscribers, their existing controls are reviewed as part of a larger incident management framework and new controls are added as appropriate.

All Code subscribers should have clearly defined roles and responsibilities around data and privacy breaches. This enables effective communication between various departments to ensure privacy and data breaches are less likely to be overlooked and takes on the recommendation from the 2018 OMI privacy compliance checklist.

Almost all Code subscribers have clear Data Breach Response Plans (DBRP) in place with a clear list of key roles and responsibilities for managing privacy and data breaches or issues relating to them. In most cases, these procedures are approved by the board and reviewed annually. For those subscribers who do not have a board-approved policy, dedicated privacy officers are appointed by the Board to manage, delegate or provide training on privacy and data breaches. Escalation processes for managing breaches should be clear and accessible to staff. Almost all Code subscribers have a clear escalation process for staff reference.

Some of these subscribers used flow charts and visual diagrams within the compliance breach and investigation reporting process. Those without visual prompts maintained an incidents and risk events policy with concise escalation or breach reporting or had monthly prompts to report privacy breaches and incidents to the privacy officer. Smaller Code subscribers implemented a simpler approach due to their staff numbers and escalate all matters to their manager.

A data breach response plan (DBRP) should include responses for both large-scale cyber interruption as well as individual customer data breaches. A large majority of Code subscribers (87%) have policy and response plans in place and their DBRP is scaled to the nature of the breach. Most of these subscribers have internal technology compliance processes for both individual and large-scale breaches.

One respondent advised that data breaches are dealt with on a case-by-case basis and a risk assessment is conducted to measure degree and severity. Their processes are aligned with CPS 234. Two subscribers have a DBRP that only caters for individual breaches; however, they

[6] See Appendix 3, questions 6.2.10 to 6.2.14

will consider reviewing their current systems and reporting. Other subscribers indicated they were seeking external assistance to develop or review their processes to improve compliance with CPS 234.

The DBRP reinforces the accountability of organisations to protect personal information. It is critical that policies and procedures for data breach notification are implemented, compliance tested and reviewed regularly.

It is recommended that an organisation's DBRP contain a process to report a breach to the OAIC as well as notifying individuals who are at serious risk of a data breach. Most Code subscribers include step-by-step reporting to the OAIC in their processes and advise that members will be contacted via different methods of communication depending on the severity of the breach. This could mean telephone communication for smaller breaches and potentially secure email for larger breaches. A few Code subscribers (3) did not include processes to self-report to the OAIC but indicated they would determine a process if required. Their current processes do not contain the detail required to notify individual members of potential and actual data breaches.

Findings:

While most subscribers focus on staff awareness and training to prevent privacy breaches, reviewing incident and breach registers can be a useful way to identify breach trends and reduce recurrence.

To follow good practice Code subscribers should review their training and staff awareness relating to privacy regularly. This should occur at least annually to ensure that privacy breaches are reduced or unlikely to occur and to ensure staff are aware and trained to identify privacy breaches.

Code subscribers must also have a clear understanding of the Data Breach Notification practices in their organisations. This can be achieved through comprehensive training in DBRP policies and procedures.

Code subscribers should also continue to update roles and responsibilities around data and privacy breaches and consider implementing visual guides such as flow charts in their breach processes to provide staff with a quick and easy escalation process.

Code subscribers should review cyber breaches more frequently to ensure compliance with APRA's Prudential Standard CPS 234 'Information Security'[7].

Code subscribers who do not have privacy processes to self-report to the OAIC should review existing privacy processes to include OAIC reporting and clear communication procedures for notifying individuals of serious breaches to ensure compliance with requirements.

[7] See https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf

Training

Training in all aspects of privacy and data security is paramount to building information security within an organisation. It is important to review training programs after legislative and regulatory change to ensure staff have a thorough and up-to-date understanding of their privacy obligations.

Staff training[8]

An effective staff training program relating to data breaches should include how to identify a data breach, how to minimise potential data breaches and how to report data breaches. 85% of Code subscribers conduct training on the appropriate use of electronic equipment to minimise data breaches and frontline staff are provided with training on how to escalate customer reports of potential or actual fraud.

Training is usually conducted on an annual basis, and this is provided in the form of scenario workshops and online training. Training covers a range of topics including privacy principles and obligations, how to manage privacy breaches, and cyber security modules to teach about data breaches in a digital setting.

Some subscribers have also included new information technology policies to cover information storage, handling and classification. A small number of subscribers (4) do not have a current training program, however they are developing or scheduling a training program to cover this information.

A handful of Code subscribers had no explicit training arrangements for data breaches outside of the incident reporting training. However, all staff receive risk management training which covers how staff can load an operational event and include potential data breaches. There looks to be a lack of procedures on how to report data breaches and this should be included in training.

Understanding the DBRP is critical for all staff and annual privacy training material should be reviewed and updated to include questions to test staff knowledge and understanding of the DBRP. For those Code subscribers (70%) who advised they have included this in their training material, most staff are required to implement the GRC Solutions compliance training program and other e-learning modules. Privacy training modules are conducted annually, and some online training is completed by an external supplier.

Some Code subscribers have implemented an 80% pass rate for staff completing privacy e-learning. Although some subscribers haven’t updated their training to include the knowledge testing, they have all scheduled training to include the DBRP. A handful of subscribers in this group were small organisations.

[8] See Appendix 3, questions 6.3.1 to 6.3.3

Code subscribers are at varying degrees of meeting this request. They have either already implemented privacy training modules, are scheduled to include DBRP training or are reviewing their current privacy training.

Varying training methods can be useful in ensuring information is received and retained as intended. Almost all Code subscribers (97%) indicated they use a mix of formal and informal training methods. One subscriber advised that training is conducted for all staff in a number of formats including video link, branch visits, questionnaires and email updates. They also include computer-based training every two years and privacy incident analysis at staff coaching sessions.

Additional training is provided through manager meetings as well as refresher and reminder emails from risk and compliance departments. Sometimes internal audits have led to additional training to enhance privacy knowledge. Only two subscribers indicated they do not employ a range of training methods. These subscribers rely on an industry package of computer-based modules which have minimum pass levels. Additionally, privacy information is circulated to senior management.

Findings:

30% of Code subscribers do not include DBRP in their training. These Code subscribers should closely review their training modules to include DBRP to prevent potential breaches from being overlooked.

To follow good practice Code subscribers should ensure that all privacy training material is reviewed to include data breach notification, promote awareness of potential breaches and include procedures that show staff how to report data breaches.. This will ensure that staff training on privacy is enhanced. Privacy training should be consistently and regularly rolled out.

Embedding compliance into a risk framework[9]

APP 1.2 imposes a distinct, separate and constant obligation to take proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPS.

Code subscribers were asked whether they considered other ways they could embed compliance with privacy obligations into their organisation’s risk framework. Many subscribers (74%) conducted regular policy reviews to identify gaps and incorporate privacy related risks in their existing risk registers.

A good example from one subscriber was including role plays in training. Other Code subscribers mentioned CPS 234 training which covers privacy and security documentation and objectives. One Code subscriber advised that privacy compliance activity forms part of their operational risk activities and is embedded in their risk management framework. A Code subscriber described using desktop flyers regarding privacy and information security to provide guidance to staff.

[9] See Appendix 3, questions 6.3.4 to 6.3.5

Those who advised they didn’t consider other ways to embed compliance (21%) were micro or small organisations and had no privacy breaches to date. Three micro organisations advised their existing compliance programs were sufficient to manage compliance and privacy concerns.

Regular privacy reviews should be scheduled at least every two years. Almost all Code subscribers have conducted reviews within the past two years which have been completed as part of their compliance and risk function, annual internal audit plan, internal and external regular audits, quality assurance reviews or legal and risk reviews. These checks have included loan file reviews, identity documentation checks and documents supplied in relation to a Power of Attorney or deceased accounts.

A small number of subscribers (4) had no policy for privacy reviews. These Code subscribers adjust their privacy policy on an as-needs basis relating to legislative changes or GRC updates to template documents. In some instances, subscribers have been completing privacy reviews as part of other scheduled reviews and they believe this is an effective way to ensure compliance with their privacy obligations. A couple of subscribers had their privacy review incorporated into their internal audit program; however, a review has not been completed within the past two years.

Findings:

To follow good practice Code subscribers should undertake a review of their risk framework and ensure privacy compliance is incorporated in their practices to prevent breaches. They should increase staff awareness of privacy procedures and the impact of breaching privacy.

Code subscribers should incorporate a full privacy review as part of their audit scope. This needs to be improved and form part of a rotational schedule where independent review is undertaken every two years.

Review compliance[10]

Conducting a sweep of all business locations to check the adherence to a clean desk policy is one way to determine if there is a risk of privacy breaches. Only 60% of Code subscribers complete routine clean desk sweeps including access areas by cleaners, who are contractually bound to privacy policies.

Other subscribers ensure managers are accountable to conduct clean desk reviews at their branches. Staff are instructed to use locked destruction bins to prevent privacy breaches and lock screens when they walk away from their desk.

Some Code subscribers who have existing clean desk policies found breaches which were to be reported and discussed with relevant staff members. Almost a third of subscribers rely on multi-layered site access controls such as lifts, doors and building access for adequate privacy breach precaution with unofficial clean desk policies in place as well. Some Code subscribers who advised they do not have a formal policy in place performed actions similar to those with

[10] See Appendix 3, questions 6.3.6 to 6.3.11

specific policies including; secure destruction bins, paper-free environment, regular sweeps and cross checks. The questionnaire responses indicate that all Code subscribers have sufficient privacy safeguards in place and have either official or unofficial desk sweeps. Breaches are addressed directly with the employee.

Shadow shopping calls are a useful way to test privacy compliance of frontline staff when dealing with new and prospective customers. A small number of Code subscribers conduct these calls and review third party and contact centre scripts as part of their legal, risk and compliance processes.

Others conduct quality checks on recorded employee calls to confirm identification has been appropriately completed. Some subscribers advise that a minimum of two calls per month are checked for compliance obligations or shadow shopping calls are conducted by executive team members. Most Code subscribers did not have shadow shopping calls incorporated in their privacy procedures and some state that there is a strong incident reporting culture and regular communication and training instead. Staff phone monitoring was noted in most Code subscriber responses and quality assurance results are reported to senior management.

A Code subscriber’s website should include a current version of their privacy notice and policy. All Code subscribers have indicated they have this on their website. Subscribers make this accessible in a number of ways including a link to the privacy page, making the site searchable for the term ‘privacy’ and placing links in easily accessible parts of their website.

Tax file number (TFN) retention processes should be managed in line with legislation and access restricted to staff who require it as part of their role. Almost all Code subscribers check TFN retention processes, restrict access as required and mask TFNs in their database and in online applications. One subscriber advised they are restricting access to higher executive staff and are in the process of removing access from staff who do not need it as part of their role.

All Code subscribers should include an opt-out option on any customer direct marketing material to allow customers to manage the way their information is used. Most Code subscribers (87%) advised they offer an opt-out option and have this as part of a pre-formatted template, marketing checklist, bulk SMS texts, or a link/option contained within marketing material emails. Those who advised they do not include an opt-out explained this is because they conduct little to no direct marketing. For example, they may only issue a quarterly or half-yearly newsletter.

Loan balance requests are sometimes received from guarantors and it is important that correct privacy procedures are followed to prevent breaches. 65% of Code subscribers advise that requests are handled in accordance with the loan contract which requires that the borrower consents to providing information about the loan contract to the guarantor. They also advise that staff verify the identity of the guarantor before providing any information.

One Code subscriber forwards any requests of this nature to specific teams or senior lending managers. Some subscribers advised they do not accept guarantors as per their lending policies or had not received any requests of this nature. It was pleasing to see that almost all subscribers have a privacy consent policy and seek to identify the guarantor before any information is provided.

Findings:

There is no consistent adoption and monitoring of clean desk policies by Code subscribers. Such policies should be reviewed annually and be extended to common area checks, such as shared printer facilities and unsecured bins.

Temporary office accommodation should have a separate clean desk policy which provides guidelines for staff to pack up desks and place belongings in a secured locker. Privacy breach awareness should be reinforced in staff training and communications.

Only a small number of Code subscribers conduct shadow shopping as a way of measuring compliance with privacy obligations by frontline staff. Code subscribers should consider shadow shopping to help identify any gaps in training.

Alternative phone call monitoring activities should be reviewed more frequently for quality assurance and identified breaches should be addressed.

To follow good practice Code subscribers should ensure the privacy notification and policy remains easily accessible when website upgrades occur.

Code subscribers should also continue reviewing tax file number (TFN) retention processes and access restrictions. Access should only be available to staff members who require it as part of their role.

Code subscribers who send marketing material should provide an opt-out option for customers and those who issue newsletters should review their processes and content to confirm whether the newsletter is direct marketing for which an opt-out option is required. This serves to provide customers with more control over how their data is used.

Code subscribers should ensure staff follow an operational procedure regarding disclosure of information to guarantors and third-party mortgagors. The procedure should set out what information may be disclosed to a guarantor in accordance with the privacy laws, National Credit Code and COBA Code. There should also be checks in place to ensure data is not shared erroneously.

Code subscribers must continue with the strategies that are being used to evaluate the appropriateness and effectiveness of privacy practices currently being used.

To assist to review the effectiveness of processes the following four step framework for privacy compliance can be incorporated into a risk framework to ensure good privacy governance and meet ongoing compliance obligations:

1. *Embed a privacy culture*
2. *Establish effective privacy processes*
3. *Evaluate the effectiveness of these processes through monitoring and measurement*
4. *Enhance by continually improving and by being proactive, forward thinking and anticipating future challenges.*

Protecting privacy in arrangements with third parties

Third-party arrangements should be managed closely and reviewed regularly as these can be a source of privacy and security data breaches. It is expected that Code subscribers will have robust policies in place to ensure due diligence protocols and appropriate protections are prioritised in contractual agreements.

Third party review[11]

All third-party contracts should contain privacy and data breach reporting clauses to ensure protocols are followed. This Includes compliance with the Privacy Act data and breach notification. Most subscribers have processes in place to review contracts by a legal team, compliance or via a checklist prior to execution. Those that do not have these processes in place are currently reviewing their third-party contracts and updating them as required. 73% of Code subscribers have reviewed their third-party contracts considering APRA's prudential standard and CPS 234 information security guidelines.

Most of these subscribers also have the contracts reviewed by their legal team prior to execution to ensure relevant clauses are included in the contract. More than 25% of subscribers are reviewing their contracts as a result of CPS 234. However, a handful of subscribers advised they have found that it can be difficult to negotiate changes to some standard contracts.

Most Code subscribers are comfortable with current arrangements relating to third-party access to customer personal information and have regular monitoring through IT and audit departments. However, it must be noted that regular monitoring does not always prevent data breaches from parties who are not directly linked to contractual agreements. Some subscribers advised that any third-party accessing customer information is subject to a cyber/data risk assessment and contractual provisions which provide assurance on the adequacy of arrangements.

Most Code subscribers have strict contract and data security arrangements that are regularly reviewed. Some subscribers have contracts in place with third party vendors who can access personal customer information that requires them to comply with privacy obligations and report any breaches. One Code subscriber noted a trend in cyber security incidents caused by third parties. Some subscribers have advised their processes are currently under review in line with CPS 234 and some are also reviewing all third-party suppliers to ensure data security arrangements are sufficient.

Monitoring performance against agreed service level agreements (SLAs) is important when working with third party service providers. Almost all Code subscribers (92%) conduct monthly or quarterly reporting and some provide feedback to their service providers. For those subscribers who are not monitoring performance (3), they advise that reviews are performed when there is an issue and issues are not usually related to data breaches. Some third-party

[11] See Appendix 3, questions 6.4.1 to 6.4.4

contracts are reviewed annually with individual business areas undertaking reviews more frequently if performance issues arise.

Privacy impact assessments should be conducted and assessed by compliance staff to ensure there are sufficient controls in place to protect customer's information from unlawful use or disclosure. About 80% of Code subscribers conduct these assessments and some submit them to a compliance team for review. Some subscribers have indicated they undertake privacy impact assessment as part of new projects or when significant operational changes occur. These assessments are undertaken in line with the Australian Privacy Principles. For those subscribers who do not conduct these assessments, they have indicated this is because they have limited, or no third parties associated with their business. However, they do incorporate the assessment as part of their annual reviews. Some subscribers have advised that their processes are currently under review in line with CPS 234 requirements.

Findings:

To follow good practice Code subscribers should conduct a complete review of contracts that involve the handling of personal information prior to execution or renewal to ensure privacy and data breach reporting standards are maintained. Checklists should be included for each contract review and Code subscribers should ensure additional consideration is given to areas assessed as having a greater risk, including the use of service providers, contractors, outsourcing and offshore storage that involves the handling of personal information.

Privacy Impact Assessment (PIA) is an effective management tool. PIAs should be undertaken for all projects or decisions that involve new or changed personal information handling practices, including implementing new technologies.

Code subscribers should incorporate due diligence protocols and appropriate protections into the terms of contracts with third parties. Code subscribers should also request third-party attestations relating to their data security.

Code subscribers should ensure there are strict contractual service level agreements in place with all third-party suppliers to ensure there are no data breaches.

Code subscribers should conduct annual reviews and regularly monitor performance of third-party contracts against agreed service levels, providing feedback to them.

Code subscribers' compliance staff should conduct privacy impact assessments to ensure there are sufficient controls in place to protect a customer's information from unlawful use or disclosure.

Conclusion

This inquiry found that the recommendations and privacy checklist provided in the 2018 OMI have not been fully implemented by all Code subscribers and that more work needs to be done to ensure ongoing compliance. As detailed in the above findings, Code subscribers may need to improve the frequency and effectiveness of privacy and data security reviews to ensure they remain compliant with Code obligations and OAIC requirements.

The Committee has determined some key focus areas for Code subscribers to improve their privacy and data security.

- Adopt formal processes to document informal actions taken within their institutions.
- Review both soft and hard copy documents to ensure information is destroyed or de-identified when no longer required.
- Consider developing a policy that details the steps required to disclose information to overseas recipients.

The recommendations outlined in this OMI should be used by Code subscribers to guide their improvements. They should also revisit the 2018 OMI for the original list of recommendations and a comprehensive privacy checklist.

APPENDIX 1: Code obligations

Customer Owned Banking Code of Practice

Key Promise 8

We will comply with our legal and industry obligations

We will be responsible, prudent managers of our institution, and will comply with all our obligations under the law and relevant codes of practice. We will act fairly and consistently with good banking and financial service industry practice.

Part D Section 23 Information privacy and security

23.1. We will comply with the Privacy Act 1988 and the Australian Privacy Principles, including with respect to credit reporting and the collection, storage, use and disclosure of your personal and financial information.

23.2. We will treat your personal and financial information as private and confidential. We will not disclose that information to any other organisation unless:

- we are required to by law (for example, under anti-money laundering laws)
- there is a duty to the public to disclose the information
- our interests require disclosure (for example, to prevent fraud)
- you ask us to disclose the information, or
- we have your permission to do so.

23.3. We will take reasonable steps to protect your personal and financial information from misuse or loss, and from unauthorised access, modification or disclosure. We will regularly review the security and reliability of our banking and payment services.

23.4. We will give you access to the information we hold on you if you ask us to, subject to certain exceptions. These are set out in our Privacy Policy and are consistent with the Australian Privacy Principles. We will correct any error that you bring to our attention. If your details change, tell us as soon as possible — we will update our records promptly.

23.5. We will make a copy of our Privacy Policy available to you on request and will publish it on our website, if we have one. We will tell you about our Privacy Policy if you ask us.

23.6. Subject to applicable laws, the commitments made in this section do not prevent us from disclosing personal and financial information to other companies in a group of companies that we belong to (where applicable).

23.7. We will comply with all applicable laws relating to the retention of your personal and financial information.

APPENDIX 2: Australian Privacy Principles

APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of 'sensitive' information.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier or use or disclose a government related identifier of an individual.

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

APP 12 — Access to personal information

Outlines an APP entity's obligations when an individual request to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.

APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

APPENDIX 3: Questionnaire results

The following questionnaire was included as section F in the 2019 Annual Compliance Statement. Questions relate to the recommendations (see Appendix 6) issued by the Committee in its previous own motion inquiry report published in June 2018.

Table 1: Questionnaire results

Code subscriber size by $ in assets	***Under $200m***	***$200 to $500m***	***$500 to $1b***	***$1b to $2b***	***Over $2b***	***Total***
6.1 Review						
6.1.1 Did you review your privacy and data security policy and practices in the past 12 months? Please provide date of last review.						
Yes	18	11	10	8	12	59
No	1	-	1	-	-	2
Other	-	-	-	1	-	1
6.1.2 Following the outcomes of your review, have you updated the appropriate policies and procedures?						
Yes	15	9	10	8	10	52
No	4	1	-	-	-	5
Other	-	1	1	1	2	5
6.2 Key areas for consideration						
6.2.1 Is your Privacy Policy easily available to customers and potential customers?						
Yes	19	11	11	9	12	62
6.2.2 Do both your hard copy and online customer application processes include your Privacy Notification?						
Yes	11	11	11	9	12	54
No	4	-	-	-	-	4
Other	4	-	-	-	-	4
6.2.3 Have you considered use of a standard privacy oral consent script and/or a pre-recorded message to capture the first time you talk to potential customers?						
Yes	2	5	5	6	10	28

Code subscriber size by $ in assets	*Under $200m*	*$200 to $500m*	*$500 to $1b*	*$1b to $2b*	*Over $2b*	*Total*
No	15	5	6	1	2	29
Other	2	1	-	2	-	5
6.2.4 Does your Privacy Policy address how you deal with overseas disclosures?						
Yes	14	9	10	9	12	54
No	3	1	1	-	-	5
Other	2	1	-	-	-	3
6.2.5 Are your staff access levels to the banking system and internal documents reviewed regularly, ideally annually? Are they up-to-date and consistent with all job descriptions?						
Yes	19	11	10	9	11	60
Other	-	-	1	-	1	2
6.2.6 Is your password protocol strong and are you sure that staff never share passwords?						
Yes	17	11	11	9	11	59
Other	2	-	-	-	1	3
6.2.7 Have you conducted an audit on the physical access at all locations?						
Yes	12	9	9	7	11	48
No	5	2	2	-	-	9
Other	2	-	-	2	1	5
6.2.8 Review your retention practices for both soft and hard copy documents for each department. Do you have processes and procedures in place to ensure that all information is destroyed and/or de-identified when no longer required?						
Yes	19	11	10	8	9	57
Other	-	-	1	1	3	5
6.2.9 Review any off-site storage and scanning processes. Do you have destruction protocols in place?						
Yes	15	9	10	9	11	54
No	1	-	1	-	-	2
Other	3	2	-	-	1	6

Code subscriber size by $ in assets	*Under $200m*	*$200 to $500m*	*$500 to $1b*	*$1b to $2b*	*Over $2b*	*Total*
6.2.10 Review your incident and breach register and look for privacy breach trends. Are there any controls that can be added to reduce recurrence?						
Yes	6	6	9	5	9	35
No	8	4	2	4	-	18
Other	5	1	-	-	3	9
6.2.11 Do you have privacy and data breach roles and responsibilities clearly defined within a Board-approved policy?						
Yes	19	10	10	9	12	60
Other	-	1	1	-	-	2
6.2.12 Do you have a clear escalation process that staff can refer to (a flow chart is a good visual guide)?						
Yes	17	9	11	8	11	56
No	2	-	-	-	-	2
Other	-	2	-	1	1	4
6.2.13 Does your Data Breach Response Plan (DBRP) cater for both large-scale cyber interruption and individual customer data breaches?						
Yes	13	10	11	9	11	54
No	2	-	-	-	-	2
Other	4	1	-	-	1	6
6.2.14 Does your DBRP include your process to report to the Office of the Australian Information Commissioner (OAIC) and how you will notify individuals at serious risk of a data breach?						
Yes	13	11	10	9	11	54
No	2	-	1	-	-	3
Other	4	-	-	-	1	5
6.3 Training						
6.3.1 Have you implemented a staff training program that includes how to identify a data breach, how to minimise potential data breaches and how to report data breaches?						
Yes	16	9	9	8	11	53

Code subscriber size by $ in assets	*Under $200m*	*$200 to $500m*	*$500 to $1b*	*$1b to $2b*	*Over $2b*	*Total*
No	3	1	-	-	-	4
Other	-	1	2	1	1	5
6.3.2 Have you ensured your annual privacy training material is updated to include questions to test staff knowledge and understanding of the DBRP?						
Yes	11	8	8	7	10	44
No	6	3	1	2	-	12
Other	2	-	2	-	2	6
6.3.3 Have you considered using a mix of formal and informal training methods such as face-to-face, e-learning, in-house and external training sessions, intranet resources, staff meetings, reminder emails and quizzes?						
Yes	19	10	10	9	12	60
No	-	1	-	-	-	1
Other	-	-	1	-	-	1
6.3.4 Have you considered other ways you can embed compliance with privacy obligations into your company's risk framework?						
Yes	11	6	10	7	12	46
No	5	5	1	2	-	13
Other	3	-	-	-	-	3
6.3.5 Do you have regular privacy reviews scheduled? Has a review been conducted within the past two years?						
Yes	17	10	11	7	11	56
No	2	1	-	1	-	4
Other	-	-	-	1	1	2
6.3.6 Conduct a 'clean desk policy' sweep of all business locations. Is any personal information left in plain sight? (Remember to check waste bins and all public areas)						
Yes	12	6	8	4	7	37
No	5	5	2	5	2	19
Other	2	-	1	-	3	6

Code subscriber size by $ in assets	*Under $200m*	*$200 to $500m*	*$500 to $1b*	*$1b to $2b*	*Over $2b*	*Total*
6.3.7 Have you undertaken some shadow shopping calls? Are staff in all front-line situations following your privacy notification requirements for new and potential customers?						
Yes	3	2	2	4	5	16
No	12	9	8	5	6	40
Other	4	-	1	-	1	6
6.3.8 Does your website include the current versions of your Privacy Notification and Policy? Are they easy to find?						
Yes	19	11	11	9	12	62
6.3.9 Check your Tax File Number (TFN) retention processes. Is access restricted to staff whose role specifically requires access?						
Yes	19	11	10	9	12	61
Other	-	-	1	-	-	1
6.3.10 Do you always include an opt-out option on any customer direct marketing material you distribute electronically?						
Yes	12	10	11	9	12	54
No	2	-	-	-	-	2
Other	5	1	-	-	-	6
6.3.11 How do your staff handle a loan balance request from a guarantor?						
Requests are handled in accordance with loan contract	12	7	8	8	5	40
Requests are handled by specific team	-	1	-	-	-	1
Other (e.g. do not accept guarantors as per lending policies, have not received such a request)	7	3	3	1	7	21
6.4 Protecting privacy in arrangements with third parties						
6.4.1 Are the privacy and data breach reporting clauses in each third-party contract sufficient?						
Yes	16	8	7	7	7	45
No	1	1	1	1	-	4

Code subscriber size by $ in assets	*Under $200m*	*$200 to $500m*	*$500 to $1b*	*$1b to $2b*	*Over $2b*	*Total*
Other	2	2	3	1	5	13
6.4.2 Are you comfortable with the third-party access to customer personal information and their data security arrangements?						
Yes	19	9	10	8	9	55
No	-	-	-	-	1	1
Other	-	2	1	1	2	6
6.4.3 Are you regularly monitoring performance against the agreed Service Level Agreements?						
Yes	16	11	11	9	10	57
No	3	-	-	-	-	3
Other	-	-	-	-	2	2
6.4.4 Do you conduct a privacy impact and risk assessment prior to engaging with third-party contractors or services that include exposure to customer's personal information?						
Yes	13	10	8	9	10	50
No	2	1	2	-	-	5
Other	4	-	1	-	2	7

APPENDIX 4: Privacy breach and complaints data over past five years

Table 2: Self-reported Code breach data concerning privacy obligations

Size $ in assets	Under $200m	Between $200m and $500m	Between $500m and $1b	Between $1b and $2b	Over $2b	Grand Total	In % of total self-reported Code breaches
KP8 We will comply with our legal and industry obligations							
2018-19	2	50	48	7	204[12]	311	15%
2017-18	5	0	61	268[13]		334	17%
2016-17	1	19	20	98[14]		138	11%
2015-16	n/a	n/a	n/a	n/a		132	16%
2014-15	n/a	n/a	n/a	n/a		111	17%
D23 Information privacy and security							
2018-19	5	51	60	16	393[15]	525	26%
2017-18	9	14	18	394[16]		435	22%
2016-17	15	15	31	233[17]		294	24%
2015-16	n/a	n/a	n/a	n/a		249	30%
2014-15	n/a	n/a	n/a	n/a		131	20%

Table 3: Self-reported internal dispute resolution data concerning privacy

Size $ in assets	Under $200m	Between $200m and $500m	Between $500m and $1b	Between $1b and $2b	Over $2b	Grand Total	In % of total self-reported IDR complaints
2018-19	2	19	15	27	420[18]	483	2%
2017-18	2	7	26	270[19]		305	2%
2016-17	17	7	35	164[20]		223	1%
2015-16	n/a	n/a	n/a	n/a		118	1%
2014-15	n/a	n/a	n/a	n/a		103	1%

[12] 155 (76%) breaches self-reported by three Code subscribers in that category
[13] 185 (69%) breaches self-reported by three Code subscribers in that category
[14] 39 (40%) breaches self-reported by one Code subscriber in that category
[15] 248 (63%) breaches self-reported by four Code subscribers in that category
[16] 274 (70%) breaches self-reported by five Code subscribers in that category
[17] 70 (30%) breaches self-reported by one Code subscriber in that category
[18] 344 (82%) IDR complaints self-reported by two Code subscribers in that category
[19] 163 (60%) IDR complaints self-reported by two Code subscribers in that category
[20] 70 (43%) IDR complaints self-reported by one Code subscriber in that category

APPENDIX 5: Participating Code subscribers

Table 4: Participating Code subscribers

	Size of Code subscriber (measured by $ amount in assets)					
	Under $200m	*$200m to $500m*	*$500m to $1b*	*$1b to $2b*	*Over $2b*	*Total*
Number of active members						
Up to 10,000	17	1	0	0	0	***18***
Between 10,000 and 50,000	2	9	10	5	0	***26***
Between 50,000 and 100,000	0	1	1	4	4	***10***
Between 100,000 and 200,00	0	0	0	0	3	***3***
Over 200,000	0	0	0	0	5	***5***
Number of full-time equivalent staff						
Up to 20	16	1	0	0	0	***17***
Between 21 and 30	1	1	0	0	0	***2***
Between 31 and 50	2	6	2	0	0	***10***
Between 51 and 100	0	2	6	2	0	***10***
Over 100	0	1	3	7	12	***23***
TOTAL	***19***	***11***	***11***	***9***	***12***	***62***

APPENDIX 6: Recommendations from 2018 Inquiry Report

In June 2018, the Committee published its findings regarding a review of customer owned banking institutions' compliance with privacy obligations under Section 23 and Key Promise 8 of the Code. A copy of the report can be found here[21].

As part of its report, the Committee published the following recommendations and privacy checklist.

Recommendations

Open banking and the future of privacy

1. In the open banking environment, institutions' data storage and transfer processes and procedures should be updated to address the increased risk of hacking and unauthorised access.
2. Institutions should proactively monitor their compliance with privacy obligations, rather than relying exclusively on customer complaints to identify issues.

Collecting personal information

3. Institutions should prevent the collection of unnecessary or irrelevant information.
4. Institutions should have appropriate processes for seeking consent, preferably written consent for the collection of sensitive information.
5. Institutions need processes and procedures for destroying unsolicited and unnecessary information.

Managing personal information

6. Institutions should ensure that password protocols are strong, and that staff never share passwords.
7. Institutions should have a clean desk policy.
8. Institutions should ideally have banking system restrictions in place.
9. Institutions should have robust processes and procedures for verifying the identity of persons requesting access to personal information.
10. Institutions should review the adequacy of their security arrangements at least annually.
11. New processes and technologies should prompt privacy impact and risk assessments before any third-party contractors are engaged.
12. Institutions should systematically review their privacy and security settings. This should include – but not be limited to – testing security settings.

[21] See http://www.cobccc.org.au/uploads/2018/06/COB-OMI_Privacy-26June2018.pdf

13. Manual reviews and spot checks should be supplemented by regular system-wide reviews of data accuracy. Where appropriate, they should use information from third parties and other sources to update customer information.
14. Institutions should take reasonable steps to confirm and correct information, including contacting customers. They should check that inaccurate, out-of-date, incomplete, irrelevant or misleading information has not impacted the customer or third parties before removing it from the system.
15. Institutions should have a policy and processes for destroying or de-identifying unneeded information, including digital information.

Using personal information

16. Institutions should ensure their privacy procedures cover how information can be used for direct marketing and when it can be disclosed to other parties, as well as how customers can access their own data.
17. Institutions should follow good practice by making direct marketing an opt-in choice. At a minimum, they must have clear, plain English avenues for opting out.
18. Institutions should specifically develop privacy consents to support understanding, using concise, plain English expression and user-friendly design.
19. Institutions should review their privacy consent processes considering open banking requirements.
20. Institutions should develop processes for providing written refusal of a customer's request for access to information.
21. Institutions should review their compliance with privacy requirements on information disclosure to guarantors. They should only provide information concerning the loan, including the current balance of the debtor's account; any amounts credited or debited during a period specified in the request; any amounts currently overdue and the dates they became due; and any amount currently payable and the date it becomes due. They must not provide information about a customer's transaction or savings accounts.

Managing compliance with privacy obligations

22. Institutions should provide ongoing and refresher training, as well as routine staff alerts and reminders of privacy obligations to all staff that have contact with customer personal information.
23. Institutions should conduct a comprehensive privacy review annually.
24. Institutions should ensure that there are strict contractual Service Level Agreements (SLAs) in place with all third-party suppliers that have access to customer information and that these are regularly monitored of performance against the agreed SLAs. Examples of third parties include customer statement printers, IT software providers, external help desks, auditors, etc.

25. Institutions should review how they deal with overseas disclosure.

26. Institutions should ensure that their privacy policies are visible and readily accessible to customers.

Privacy compliance checklist

1. Review privacy source materials.

Source materials for review include:

- Office of the Australian Information Commissioner (OAIC) guides such as *A Guide to Handling Personal Information Security Breaches*
- COBA's *Record Retention – a Guide to your Legal Obligations* (May 2016)
- COBA's *Australian Privacy Principles Compliance Manual* (February 2018)

2. Review your privacy policy, privacy notification and process for obtaining consent.

- Is your Privacy Policy easily available to customers and potential customers?
- Ensure both your hard copy and online customer application processes include your Privacy Notification.
- Consider use of a standard privacy oral consent script and/or a pre-recorded message to capture the first time you talk to potential customers.
- Does your Privacy Policy address how you deal with overseas disclosures?

3. Review data security and integrity.

- Review staff access levels to the banking system and internal documents regularly, ideally annually. Are they up to date and consistent with all job descriptions?
- Is your password protocol strong and are you sure that staff never share passwords?
- Have you conducted an audit on the physical access at all locations?

4. Review retention and deletion/de-identification of personal information.

- Review your retention practices for both soft and hard copy documents for each department. Do you have processes and procedures in place to ensure that all information is destroyed and/or de-identified when no longer required?
- Review any off-site storage and scanning processes. Do you have destruction protocols in place?

5. Review breaches and determine trends and additional controls.

- Review your incident and breach register and look for privacy breach trends. Are there any controls that can be added to reduce recurrence?

- Review the last COBCOBP Annual Report breaches – can you learn any lessons from other's experiences and remediation plans?

6. Review compliance with privacy spot checks.

- Do you have regular privacy reviews scheduled? Has a review been conducted within the last two years?
- Conduct a clean desk policy sweep of all business locations. Is any personal information left in plain sight? Remember to check waste bins and all public areas.
- Make some shadow shopping calls. Are staff in all front-line situations following your privacy notification requirements for new and potential customers?
- Does your website include the current versions of your Privacy Notification and Policy? Are they easy to find?
- Check your TFN retention processes. Is access restricted to staff whose role specifically requires access?
- Do you always include an opt-out option on any customer direct marketing material you distribute electronically?
- How do your staff handle a loan balance request from a guarantor?

7. Ensure you have a compliant Data Breach Response Plan (DBRP).

- Ensure you have privacy and data breach roles and responsibilities clearly defined within a Board-approved policy.
- Have a clear escalation process that staff can refer to (a flow chart is a good visual guide).
- Ensure your DBRP caters for both large scale cyber interruption and individual customer data breaches.
- Ensure your DBRP includes your process to report to the OAIC and how you will notify individuals at serious risk of a data breach.

8. Raise staff awareness of privacy requirements and your DBRP.

- Implement a staff training program that includes how to identify a data breach, how to minimise potential data breaches and how to report data breaches.
- Ensure your annual privacy training material is updated to include questions to test staff knowledge and understanding of the DBRP.
- Consider using a mix of formal and informal training methods – face-to-face, e-learning, in-house and external training sessions, intranet resources, staff meetings, reminder emails and quizzes.

- Consider what other ways you can embed compliance with privacy obligations into your company's risk framework.

9. Consider your third-party contracts.

- Are the privacy and data breach reporting clauses sufficient?
- Are you comfortable with the third-party access to customer personal information and their data security arrangements?
- Are you regularly monitoring performance against the agreed Service Level Agreements?

10. Ensure that new processes and technology are privacy compliant.

- Ensure you conduct a privacy impact and risk assessment prior to engaging with third-party contractors or services that include exposure to customer's personal information.

11. Embed changes into your relevant policies and procedures.

- Following the outcomes of the steps above update the appropriate policies and procedures, including (but not limited to):
    - Privacy Program, Policy and Notifications
    - Staff Training Policy and Programs
    - Business Continuity Plan and Policy
    - Data Breach Policy
    - Outsourcing Policy
    - Incident Management Policy
    - Customer Complaints Policy

APPENDIX 7: About the Code and the Committee

The Code

The Customer Owned Banking Code of Practice (the Code) was developed by the Customer Owned Banking Association (COBA) and commenced operation on 1 January 2014. The Code replaces the 2010 Mutual Banking Code of Practice.

The Code has been revised to accommodate changes the Australian Securities and Investments Commission (ASIC) made to Regulatory Guide 221[22] *Facilitating digital financial services disclosures* and the *e-Payments Code*. The revised Code has been effective from 1 July 2016. A further update was published, effective 1 January 2018.

Through the Code, 62 subscribing[23] credit unions, mutual banks and mutual building societies voluntarily commit to fair and responsible customer owned banking.

The Committee

The Code Compliance Committee (the Committee) is an independent compliance monitoring body established under the Code and the Code Compliance Committee Charter (the Charter). It comprises an independent chair, a person representing the interests of the customer owned banking sector and a person representing the interests of consumers and communities.

The purpose of the Committee is to encourage and promote customer owned banking Code subscribers to meet customer and community needs and expectations.

To achieve this, the Committee monitors Code compliance, share recommendations for good practice, engage with stakeholders, analyse the external financial services' environment and ensure efficient and effective Committee operations.

For more information about the Code and the Committee, please visit www.cobccc.org.au.

Customer Owned Banking Code Compliance Committee

PO Box 14240 Melbourne VIC 8001

email: info@codecompliance.org.au

Phone: 1800 931 678 (free call - please ask for 'Code Compliance')

www.cobccc.org.au

[22] See https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-221-facilitating-digital-financial-services-disclosures/

[23] Number of Code subscribers as at June 2019.