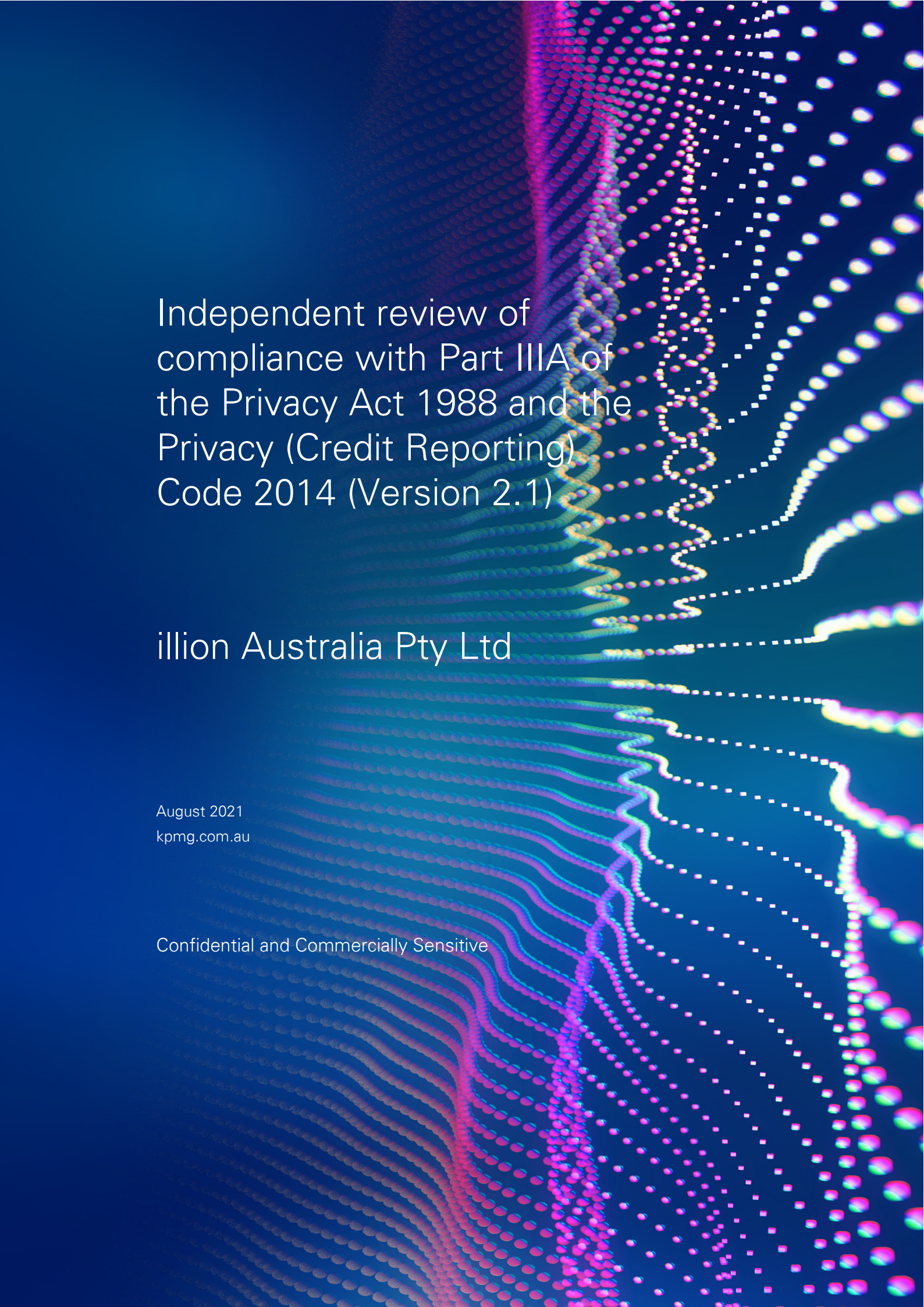

Independent review of compliance with Part IIIA of the Privacy Act 1988 and the Privacy (Credit Reporting) Code 2014 (Version 2.1)

illion Australia Pty Ltd

August 2021

kpmg.com.au

Confidential and Commercially Sensitive

Inherent Limitations

*As set out in our Engagement Letter dated 06 May 2021 (**Engagement Letter**), KPMG has undertaken an independent review of illion Australia Pty. Ltd's (**illion**) compliance with Part IIIA of the Privacy Act 1988 (**Privacy Act**) and the Privacy (Credit Reporting) Code 2014 (Version 2.1) (**CR Code**) (**the Engagement**).*

The services provided in connection with the Engagement comprise an advisory engagement, which is not subject to assurance or other standards issued by the Australian Auditing and Assurance Standards Board and consequently no opinions or conclusions intended to convey such assurance have been expressed.

No warranty of completeness accuracy or liability is given in relation to the statements and representations made by, and the information and documentation provided by illion or illion management and personnel consulted as part of the process.

KPMG has indicated within this Report the sources of the information provided. We have not sought to independently verify those sources unless otherwise noted within the Report. KPMG has not, and is not obliged, to undertake any procedures in relation to, or update this Report for events occurring subsequent to 10 August 2021 that may be relevant to this Report.

Due to the inherent limitations of any internal control structure, it is possible that fraud, error or non-compliance with laws and regulations may occur and not be detected.

Further, the internal control structure within which the control procedures that have been subject to the procedures we have performed, has not been reviewed in its entirety, and therefore, no opinion or view is expressed as to the effectiveness of the greater internal control structure. The procedures performed were not designed to detect all weaknesses in control procedures as they were not performed continuously throughout the period and the tests performed on the control procedures were performed on a sample basis. Any projection of the evaluation of control procedures to future periods are subject to the risk that the procedures may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

The findings of this Report have been formed on the above basis.

Third Party Reliance **[updated]**

This Report has been prepared solely for the purpose set out in Part 1 and for illion and the OAIC's information and is not to be used for any other purpose or distributed to any other party without KPMG's prior written consent. This Report has been prepared at the request of illion in accordance with the terms of KPMG's Engagement Letter dated 06 May 2021 and is not to be used for any other purpose. We consent to this report being released to the OAIC on the basis set out in our Engagement Letter and, whilst it is recognised that a copy of this report will also be available on illion's website, other than our responsibility to illion, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this Report. Any reliance placed is that party's sole responsibility.

We disclaim any assumption of responsibility by KPMG to any person other than illion, or for any use of this Report for any purpose other than that for which it was prepared.

The definitive version of this Report is the one bearing our original signature and illion management is responsible for any errors or in accuracies appearing in any reproduction in any form or medium.

Contents

1 Executive summary

1.1 Introduction

illion Australia Pty. Ltd (**illion**) is a Credit Reporting Body (**CRB**) under the Privacy Act 1988 (**Privacy Act**) and accordingly collects, uses, and discloses personal information in the conduct of its credit reporting business. As a result, the information that illion collects, uses, and discloses is regulated under the Privacy Act and the Privacy (Credit Reporting) Code 2014 (Version 2.1) (**CR Code**). This report considers those obligations only and not the Australian Privacy Principles.

As set out in our Engagement Letter dated 06 May 2021, KPMG has undertaken an independent review of illion's compliance with the Privacy Act, the Regulations and the CR Code and produced two KPMG branded reports – an "external report" including a summary of compliance status and remediation action plan (if required) and a "detailed report" including detailed testing description and remediation action plan (if required). Accordingly, this detailed report contains our conclusive findings and detailed testing description.

1.2 Background

In accordance with paragraph 24.2 of the CR Code, every three years (or more frequently, if the Commissioner requests), a CRB must commission an independent review of its operations and processes to assess compliance by the CRB with its obligations under the Privacy Act, the Regulations and the CR Code. In addition, the CRB must consult with the Commissioner as to the choice of reviewer and scope of the review. The review report and the CRB's response to the review report must be provided to the Commissioner and made publicly available.

illion engaged KPMG to undertake the independent review of its Privacy Framework's design and operating effectiveness for compliance with the Privacy Requirements. This review is necessarily a point in time review focusing on the Privacy Framework of the illion credit reporting business entity.

1.3 Scope

The scope of the Engagement is agreed as follows:

- A current state assessment of governance, policies, and processes to manage the credit information lifecycle (e.g. collect, use, disclose, store, etc.);
- Testing over the process and controls that illion has implemented to ensure compliance under the Privacy Act, the Regulations and the CR Code; and
- Reporting the findings and observations in addition to an action plan (if required) in accordance with the obligations under the Privacy Act, the Regulations, and the CR Code (collectively, **Scope**).

1.4 Limitations

This report and the opinions expressed in this report are subject to the following limitations:

1. The services provided in connection with this engagement comprise an advisory engagement, which is not subject to assurance and other standards issued by the Australian Auditing and Assurance Standards Board and, consequently, no opinions or conclusions intended to convey assurance have been expressed. Had we performed additional procedures or had we performed an audit in accordance with Australian Auditing Standards or a review in accordance with Australian Auditing Standards applicable to review engagements, other matters might have come to our attention that would have been reported to you. Observations made are founded on our interpretation of the Privacy Act, the Regulations and the CR Code and other guidelines, which may differ from the subsequent interpretation of those laws, regulations, and guidelines by OAIC.
2. KPMG does not warrant the accuracy or reliability of any of the information supplied to it in the course of this engagement.
3. Any redistribution of this report requires written approval of KPMG and, in any event, is to be a complete and unaltered version of the report and accompanied only by such other materials as KPMG may agree.
4. Review of the Information Security Management System (**ISMS**) and Business Continuity Management System framework (**BCMS**) is not part of the scope.
5. Responsibility for the security of any electronic distribution of this report remains the responsibility of illion.
6. Due to COVID-19, KPMG did not perform any physical walkthrough of the illion premises to assess the physical security and related data handling controls.
7. KPMG accepts no liability if the report is or has been altered in any way by any person.
8. KPMG's role does not include any explicit or implicit approval functions or responsibilities.

2 Approach

2.1 Summary of approach

In light of the Scope, the approach was broken down into the following four steps:

- Step 1: Initial Diagnostic;
- Step 2: Review of Governance and Processes;
- Step 3: Testing of Process Controls; and
- Step 4: Reporting and Review of Action Plan.

[KPMG proprietary methodology withheld]

[KPMG proprietary methodology withheld]

3 Overall Conclusion

Overall, the design of illion's operations and control processes is compliant with its obligations under the Privacy Act, the Regulations, and the CR Code. It was evident during our review that there is strong awareness and knowledge within illion's employees of the business' obligations under the Privacy Act, the Regulations, and the CR Code, which is consistent with the overarching policies and procedures at illion and reiterate its compliance obligations. illion has robust processes and systems to ensure that the credit information it uses and discloses is in line with the requirements of the Privacy Act, the Regulations, and the CR Code. illion also has adequate controls to address its obligations to provide access, correct information, and handle complaints as per the obligations under the Privacy Act, the Regulations, and the CR Code. Our review identified two minor improvement opportunities in relation to illion's practices relating to the use and destruction of credit information. These have been discussed with illion management who are committed to addressing these.

3.1 Compliance Status

The following table outlines the compliance status indicator used throughout this report, compliance status, and corresponding descriptions.

Compliance Status Indicator	Compliance Status	Description
	Compliant	No exception noted or minor improvement opportunity noted.
	Minor Non - Compliant	A minor exception to the Privacy Act, the Regulations, and/or the CR Code requirements noted.
	Non - Compliant	An exception to the Privacy Act, the Regulations, and/or the CR Code requirements noted.

The below table summarises illion's compliance against the relevant sections / paragraphs of the Privacy Act, the Regulations and the CR Code.

Report Ref.	Part IIIA Ref.	CR Code Ref.	Subdivision	Compliance Status
4.1	Section 20 B	Para 2, 3	Subdivision B – Consideration of information privacy	Minor improvement opportunity noted *B.20B.0.2* *(Refer to Section 3.2)*
4.2	Sections 20C, D & L	Para 5, 6, 7, 8, 9, 10, 11 and 12	Subdivision C – Collection of credit information	No exception noted
4.3	Sections 20 E, F, G, H, J & M, P, 20K	Para 7, 8, 9, 12,14,16, 17 and 22	Subdivision D – Dealing with credit reporting information	No exception noted
4.4	Sections 20 N & Q	Para 2, 5, 15 and 23	Subdivision E – Integrity of credit reporting information	No exception noted
4.5	Sections 20 R, S, T, U & Div 5 S23	Para 19, 20 & 21	Subdivision F – Access to and correction of information	No exception noted
4.6	Sections 20 B, J, V, W, X, Y, Z & ZA	Para 1.2 and 22	Subdivision G – Dealing with credit reporting information after the retention period ends	Minor improvement opportunity noted *G.20V.0.2* *(Refer to Section 3.2)*
4.7	N/A	Para 24	Additional requirement: Independent review of compliance	No exception noted

3.2 Summary of Improvement Opportunities

The following table below presents the three improvement opportunities identified during this review, along with illion's comments. Section 4 provides further details of all the Privacy Act, the Regulations and the CR Code obligations we assessed illion's operations and processes against as they apply to illion, including a summary of those obligations. Our review was conducted by reference to the applicable obligations rather than the summary included in the next part of this report.

Report Ref.	Details of the Improvement Opportunities	illion Comments
B.20B.0.2	Document/Version history is missing from some of the illion policy/process documents.	illion acknowledges this and will address to ensure regular reviews and updates are recorded correctly.
G.20V.0.2	Although the physical document disposal process exists in practice, it has not been formally documented by illion.	illion will action this by ensuring the existing process is correctly documented.

4 Findings

The following table sets out:

- The relevant obligations of the Privacy Act, the Regulations and the CR Code;
- A description of the testing performed; and
- Our assessment of the compliance status for each relevant obligation.

4.1 Subdivision B – Consideration of information privacy

20B: Open and transparent management of credit reporting information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
B.20B.0.1	Div 2, Sec 20B (3) & (4)	Para 3	illion must have a clearly expressed and up-to-date policy about the management of its credit reporting information, which must contain information as required by the Privacy Act, including the following: • the kinds of credit information collected and methods of collection; • the kinds of credit reporting information held and how information is held; • how personal information is derived from credit information illion holds; • the purposes for which illion collects, holds, uses, and discloses credit reporting information; • information about the effect of the use or disclosure of credit reporting information for the purposes of	Inspected the Credit Reporting Policy (**CRP**) and noted it contains all required elements.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			direct marketing, and how an individual can request to not use their information for pre-screening purposes; • how an individual may access credit reporting information about themselves and seek correction of such information; and • how an individual may complain about a failure of illion to comply with Division 2 or the registered CR Code and how illion will deal with the complaint.		
B.20B.0.2	Div 2, Sec 20B (2)	Para 3	illion must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to its credit reporting business that will ensure that illion complies with its credit reporting obligations under the Privacy Act and the CR Code. illion has credit reporting related policies, processes and procedures documented and has them periodically reviewed.	Inspected all the credit reporting information-related policies, processes, and procedures and noted that these provide guidelines and steps to be followed while using, disclosing, retaining, storing, archiving, managing integrity, security, quality of credit information. Further, it was noted that document/version history was not included in the following process/procedure documents: 1. Complaint Handling Procedure (internal) 2. Ban Application Process	 Minor improvement opportunity noted. *Refer to Section 3.2.*
B.20B.0.3	Div 2, Sec 20B (5)	Para 3 & 3.1	illion must make its Credit Reporting Policy available for free and publish the policy on its website.	Inspected the availability of the CRP on the illion website (https://www.illion.com.au/illion-credit-reporting-policy-australia/) and noted that the CRP is available for free.	
B.20B.0.4	Div 2, Sec 20B (2)	Para 3	illion must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to its credit reporting business that will ensure that illion complies with its credit reporting obligations under the Privacy Act and the CR Code.	Inspected the Privacy Compliance Officer role description (Privacy Compliance Officer role PD). Held discussions with the Privacy Compliance Officer and noted that the assigned Privacy Compliance Officer oversees the activities listed in the Summary of Obligations.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			illion has an assigned officer (e.g. privacy officer) with clear responsibility for ensuring compliance with credit reporting obligations. The role description for the assigned officer covers the following activities: • monitoring compliance with credit reporting obligations under the Privacy Act and the CR Code; • conducting, or assisting in, third party oversight in relation to credit reporting; • training staff; • ensuring performance of audit activity relating to credit reporting; • developing, implementing, and maintaining privacy policies and procedures; • oversight of the investigation, tracking, and resolution of credit reporting incidents, breaches, complaints, and enquiries; • ownership of internal and external policies relating to credit reporting and responsibility for reporting on its operation to the Board or senior Executive in line with your entity's stated risk appetite; • responsibility for reporting to the Board or senior Executive on the operation credit reporting policies and processes, in line with your CRB's stated risk appetite; • providing additional reports and monitoring, as appropriate; • liaising with relevant business units within your CRB (e.g. legal, risk, IT, privacy);		

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			• liaising with relevant credit reporting bodies; and • cooperating with appropriate regulators.		
B.20B.0.5	N/A	Para 2.2 (a),(b)	illion must take reasonable steps to: • inform employees who handle credit reporting information of the requirements of Part IIIA, the Regulations and the CR code; and • train employees who handle credit reporting information in the practices, procedures, and systems that are designed to achieve compliance with those requirements.	Inspected Credit Reporting training documents, held stakeholder consultations, and noted that the Credit Reporting training covers topics including (but not limited to) rules relating to consumer credit information and commercial credit information, timeframes and processes for access, correction and complaints from customers, the role of the regulator, and information relating to the credit reporting system including the roles of Credit Providers (**CP**s) and Credit Reporting Bureau (**CRB**). Further, during stakeholder discussions it was noted that all employees dealing with credit reporting information receive Credit Reporting mandatory training, and completion rates are monitored and enforced (including some staff having performance tied directly to training completion). Inspected Credit Reporting training documents, held stakeholder consultations and noted that the Credit Reporting training covers required topics including (but not limited to) rules relating to consumer credit information and commercial credit information, including timeframes for access, correction, and complaints from customers, the role of the regulator. Further, during stakeholder discussions it was noted that all employees dealing with credit reporting information receive this mandatory training, and completion rates are monitored and enforced (including some staff having performance tied directly to training completion).	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
B.20B.0.6	Div 2, Sec 20B (2)	Para 3	illion must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to its credit reporting business that will ensure that illion complies with its credit reporting obligations under the Privacy Act and the CR Code. Credit reporting risks are included in illion's risk statement.	Inspected the illion Risk Management Policy and noted that it includes a risk appetite relating to risks resulting from services in areas of consumer credit and credit bureaus. Stakeholders confirmed that the risk register is updated and tracked regularly (quarterly, and then a deep dive annually), allocates appropriate ownership over risks and monitors closure of risks.	

4.2 Subdivision C – Collection of credit information

20C: Dealing with solicited credit information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
C.20C.0.1	Div 2, Sect 20C	Para 5.1(a), 5.2, 5.4(a), (b) & (c), 6, 7, 8, 9, 10 and 12	Unless required or authorised by or under an Australian law or a court/tribunal order, as a CRB, illion can only collect solicited credit information about an individual by lawful and fair means in the course of carrying on a credit reporting business from a CP who is permitted under section 21D of the Act to disclose the information to illion. illion may also collect credit information from an entity other than a CP, in accordance with section 20C(4). Where the information collected from a CP is:	Inspected Consumer Credit Bureau (CCB) data flow diagram and noted that illion collects consumer data from CPs, web channels, and courts/insolvency data. Inspected list of AU CCB Data Suppliers and noted that the list contains four categories of credit information providers: 1. Full Consumer Credit Reporting (**CCR**) – these are entities that supply full comprehensive credit reporting information;	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			• identification information – illion also collects from the provider, or already holds, credit information of another kind about the individual; or • consumer credit liability information – illion must not agree or implement procedures with CPs to standardise CP's numbering conventions for consumer credit, however illion must develop and maintain in conjunction with CPs common descriptors of the types of consumer credit provided to individuals. illion must have reasonable practices, procedures and systems that are designed to cover the obligations under Part IIIA, the Regulations and the CR code and in particular enable illion to: • use the information disclosed by CPs in relation to individuals' dates of birth to identify any information disclosed by a CP that: – relates to an act, omission, matter or thing that occurred or existed before the relevant individual turned 18; and – that is prohibited by Part IIIA, the Regulations or this CR code from being disclosed by the CP to illion. • as soon as practicable identify whether collected information includes information that illion is	2. Consumer Credit Liability Information (**CCLI**) – these entities supply consumer credit liability information; 3. Defaults – these entities provide default information only; and 4. Courts. During stakeholder discussion, we were advised that prior to onboarding a new CP or a new product request from a CP, credit information to be shared between the CP and illion is agreed upon. In addition, once the onboarding is completed, a project closure email is shared with the CPs. Inspected illion Consumer Schema CCR (FULL) User Guide and noted that data elements loaded in illion's CCB database (Consumer Schema) is formally documented. The illion Consumer Schema can be configured to support a variety of use cases and return different combinations of data according to customer needs. The data returned is controlled by a parameter submitted as part of the Application Programming Interface (**API**) request and referred to as a "Product Key". During the onboarding process, illion provides customers with appropriate Product Key(s) appropriate to the data they require (as agreed per the Batch Technical Documentation), and depending on which Product Key is requested in the API request, a different set of data will be returned. Inspected CCB Batch Technical Documentation and Consumer Credit Data flow diagram and noted that the	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			prohibited by Part IIIA, the Regulations or this CR code from collecting and, if so, to destroy the prohibited information; and • as soon as practicable, notify the relevant CP where illion destroys information on the basis that Part IIIA, the Regulations or this CR code prohibits illion from collecting that information.	default data loading process is formally documented. The process involves the following steps: 1) Client will build a batch default update file; 2) The batch file is then dropped into illion's SFTP server location folder; 3) The batch file is picked up by illion for processing through an automated program; 4) The batch file is processed overnight, and three Response files are generated: i) Log file (This file contains the general attribute of the file. For example: Number of records in the file, Number of records successfully processed, etc.); ii) Response file (This file contains file header, consumer header, customer transaction header, individual details, and file trailer details); and iii) Error file (This file contains information about the number of records and associated error messages because of any technical issue or data that was not agreed with CPs). 5) The above-mentioned batch response files are then placed in illion's SFTP server response folder; 6) The batch files are placed in the CPs SFTP server location folder; and 7) The batch files are then picked up by CPs to perform suitable action.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
				Inspected a sample of project closure emails and noted that the CP was informed of the: 1) Data loading outcome; and 2) Formal handover to the Business as Usual (**BAU**) operations. During stakeholder discussion, we were advised that data sourced from web channels goes through an initial data quality check and then is fed into the CCB database. Further, data received from courts is entered into the CCB database by an illion employee.	
C.20C.0.2	Div 2, Sec 20C(4)(e)	Para 8	illion is permitted to collect RHI from the CP, if the CP is a **licensee** or is prescribed by the Regulations. Where illion collects information from an entity (other than a CP), if the information is repayment history information (**RHI**) about an individual, illion collects the information from another CRB that has an Australian link.	Inspected the CR Policy and noted that illion collects repayment history from limited sources, including certain Credit Providers such as Banks and Finance Companies. Inspected a list of AU CCB Data Suppliers and noted that all suppliers have an Australian link.	
C.20C.0.3	Div 2, Sec 20L	N/A	If illion holds credit reporting information about an individual and the information is a government related identifier of the individual, illion must not adopt the government related identifier as its own identifier of the individual unless the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order.	Inspected CCB Batch Technical Documentation and noted that a unique consumer reference ID is adopted by illion to uniquely identify consumers.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
C.20C.0.4	N/A	Para 11 & 11.1	illion must only collect publicly available information about an individual: • from an agency or a state or territory authority; and • if the content of the information that is collected is generally available to members of the public (whether in the form provided to illion or another form and whether or not a fee must be paid to obtain that information); and • if the other requirements of Section 6N(k) are met, i.e: – it relates to the individual's activities in Australia or the external Territories and the individual's credit worthiness; and – it is not court proceedings information about the individual or information about the individual that is entered or recorded on the National Personal Insolvency Index (AFSA data).	Inspected the CR Policy and noted publicly available information was collected by illion, which included publicly accessible databases such as ASIC's publicly accessible databases, however the Policy provided that illion collects publicly available information that is entered or recorded on the National Personal Insolvency Index (AFSA data). Held discussions with stakeholders and noted that illion does not collect publicly available information from AFSA and the CR Policy has been updated to reflect this practice and the obligations. It was noted also that information is collected for purposes relating to an individuals' credit worthiness. Inspected credit information flow diagrams illustrating the organization's data flow and noted that illion obtains publicly available information from web channels. *Note: At the time of our testing, the CR Policy provided stated that illion collect publicly available information that is entered or recorded on the National Personal Insolvency Index (AFSA data). It was noted, however, that this did not occur in practice. We note that the CR Policy has been updated to reflect that illion does not collect information about the individual that is entered or recorded on the National Personal Insolvency Index (AFSA data).*	

20D: Dealing with unsolicited credit information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
D.20D.0.1	Div 2, Sec 20D	N/A	If illion receives unsolicited credit information about an individual, illion must, within a reasonable period after receiving the information, determine whether it could have collected the information under section 20C if illion had solicited the information. If it is determined to be unsolicited information, illion must destroy the information. If illion determines that it could have collected the credit information, illion may deal with that information as though it had collected the information. If illion determines that it could not have collected the credit information, illion must, as soon as practicable, destroy the information.	Inspected CCB Batch Technical Documentation and noted that input file requirements list the 'input' fields information that illion collects, any information that does not form part of these fields cannot be consumed by illion. It was noted that 'host restrictions' are applied to the SFTP server where the information is received. It was noted during stakeholder discussions that the 'PGP watcher' prevents unsolicited information (information types not falling within the specified 'input' fields) from getting consumed. Inspected CCB Batch Technical Documentation and Consumer Credit Data flow diagram and noted that the default data loading process is formally documented. The process involves the following steps: 1) Client will build a batch default update file; 2) The batch file is then dropped into illion's SFTP server location folder; 3) The batch file is picked up by illion for processing through an automated program; 4) The batch file is processed overnight, and three Response files are generated: i) Log file (This file contains the general attribute of the file. For example: Number of records in the file, Number of records successfully processed, etc.);	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
				ii) Response file (This file contains file header, consumer header, customer transaction header, individual details, and file trailer details); and iii) Error file (This file contains information about the number of records and associated error messages because of any technical issue or data that was not agreed with CPs). 5) The above-mentioned batch response files are then placed in illion's SFTP server response folder; 6) The batch files are placed in the CPs SFTP server location folder; and 7) The batch files are then picked up by CPs to perform suitable action. Inspected the CCB Data Quality (**DQ**) Procedure, held discussions with DQ stakeholders and noted that the data quality checks are performed across data held by illion from the initial client upload, through usage within the CCB, to deletion if necessary. It was noted that DQ checks, including but not limited to checks for 'default' common names, salacious names, similarities in names, and dummy data are performed on CCB data.	

4.3 Subdivision D – Dealing with credit reporting information

20E: Use and disclosure of credit information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
D.20E.0.1	Div 2, Sec 20E (1) & (2)	N/A	illion is permitted to use credit reporting information in the following ways: • in the course of carrying on its credit reporting business; • if the use is required or authorised by or under an Australian law or a court/tribunal order; and • if the use is a use prescribed by the regulations.	Inspected the CR Policy and noted the reasons that illion uses and discloses credit reporting information that is listed in the Policy is for the purposes set out in the Summary of Obligations.	
D.20E.0.2	Div 2, Sec 20E (5)	Para 22 (c)	illion must have a process to ensure that a written note is made of all disclosures of credit-related information. Including: (i) The date of the disclosure; (ii) A brief description of the type of information disclosed; (iii) The credit provider, affected information recipient, or other person to whom the disclosure was made; and (iv) Evidence that the disclosure was permitted under Part IIIA of the Act.	Inspected the register containing credit disclosures, held discussions with stakeholders and noted that illion records the date of disclosure, what types of information was disclosed, to whom the information was disclosed, which in turn provides evidence that the disclosure was permitted under Part IIIA of the Act.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
D.20E.0.3	Div 2, Sec 20E, 20F and 20P	Para 7, 8, 9, 12,14 and 16	illion is permitted to disclose credit reporting information about an individual if: • in relation to the individual the disclosure is a permitted CRB disclosure under section 20F. • the disclosure is to another CRB that has an Australian link. • the disclosure is for the purposes of a recognized external dispute resolution (**EDR**) scheme and illion (or the CP) is a member of the scheme. • the disclosure is to an enforcement body and illion is satisfied that the body, or another enforcement body, believes on reasonable grounds that the individual has committed a serious credit infringement. • in relation to RHI the recipient is a CP who is a licensee or is prescribed by the regulations or a mortgage insurer. The CR Code also provides the conditions under which illion can disclose certain credit information, i.e: • Para 7 – Where a CP makes an information request to illion in connection with an application for consumer credit and the amount of credit is unknown or incapable of being specified, the credit information that illion may collect and disclose may include that an	Inspected the register containing credit disclosures, held discussions with stakeholders, and noted that illion records its disclosures between CPs, mortgage insurers, and trade insurers. Inspected an email noting management comments, held discussions with stakeholders, and noted that illion does not share information with other CRBs. Inspected an Australian Financial Complaints Authority (**AFCA**) walkthrough document, held discussions with stakeholders, and noted that illion makes disclosures to AFCA and records these disclosures in a register called the AFCA complaints register, which includes the dates the case was opened and when a response is due. Inspected the RHI disclosure data extract, spreadsheet showing recipients of comprehensive data (the data set that includes RHI), held discussions with stakeholders, and noted that RHI information is only disclosed to CPs who are licenced. Inspected the register containing credit disclosures, held discussions with stakeholders, and noted data extraction shows the value of defaults is limited to amounts of $150.00 or more. Inspected sample contracts between illion and CPs and noted that clauses included obligations with regards to Privacy and the Privacy Act.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			unspecified amount of consumer credit is being sought from the CP. • Para 8 – illion is only permitted to disclose RHI to a CP that is a licensee or is prescribed by the Regulations. • Para 9 – illion is only permitted to collect and disclose default information if certain preconditions are met, including the consumer credit payment must be overdue by at least 60 days, the overdue amount must not be less that $150 (or if a higher amount is prescribed by the Regulations, that amount) and the CP must have met the notice obligations specified in Part IIIA, the Regulations and the CR Code. • Para 14 – Before illion discloses credit reporting information to a CP, mortgage insurer or trade insurer, illion must have taken reasonable steps to ensure that the CP, mortgage insurer or trade insurer has been notified of the requirements of the Privacy Act, the Regulations and the CR code governing limitations on use and disclosure of credit reporting information. • Para 16 – illion must only disclose credit reporting information to a CP, for the purposes of enabling the CP to assist the individual to avoid defaulting on his or her obligations in relation to consumer credit provided by the CP to the individual where either: – the CP confirms to illion that it is aware of circumstances that reasonably indicate that the	Inspected the batch screening specifications, batch screening user guide, held discussions with stakeholders, and noted that there is a significant risk of default filter.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			individual may be at significant risk of defaulting in relation to those obligations; or – illion is aware that an event has occurred in relation to the individual that is an event of the kind that the CP has identified could, if it were to occur, reasonably indicate that the individual may be at significant risk of defaulting in relation to those obligations.		
D.20E.0.4	Div 2, Sec 20P	N/A	illion must not use or disclose credit reporting information that is materially false or misleading, unless: • it is to determine whether unsolicited credit information received could have been collected if illion had solicited the information. • it is in consultation for the correction of credit information.	Inspected sample vendor contracts (CBA and Westpac) and noted clauses to the effect that illion must not use or disclose credit reporting information that is materially false or misleading. Inspected the CCB data flow diagram and noted that illion receives information from CPs, web channels (publicly available information), and Courts. Inspected CCB Batch Technical Documentation and Consumer Credit Data flow diagram and noted that the default data loading process is formally documented. The process involves the following steps: 1) Client will build a batch default update file; 2) The batch file is then dropped into illion's SFTP server location folder; 3) The batch file is picked up by illion for processing through an automated program;	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
				4) The batch file is processed overnight, and three Response files are generated: i) Log file (This file contains the general attribute of the file. For example: Number of records in the file, Number of records successfully processed, etc.); ii) Response file (This file contains file header, consumer header, customer transaction header, individual details, and file trailer details); and iii) Error file (This file contains information about the number of records and associated error messages because of any technical issue or data that was not agreed with CPs). 5) The above-mentioned batch response files are then placed in illion's SFTP server response folder; 6) The batch files are placed in the CPs SFTP server location folder; and 7) The batch files are then picked up by CPs to perform suitable action. Inspected the CCB Data Quality (**DQ**) Procedure, held discussions with DQ stakeholders and noted that the data quality checks are performed across data held by illion from the initial client upload, through usage within the CCB, to deletion if necessary. It was noted that DQ checks, including but not limited to checks for 'default' common names, salacious names, similarities in names, and dummy data, are performed on CCB data.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
D.20E.0.5	Div 2, Sec 20M (1) & (2)	N/A	illion may use or disclose de-identified credit reporting information in the following circumstances: • the use or disclosure is for the purposes of conducting research in relation to credit; and • illion complies with the rules made by the Commissioner which by legislative instrument, make rules relating to the use or disclosure by a credit reporting body of de-identified information for the purposes of conducting research in relation to credit.	Inspected the CR Policy and noted that research was included as a purpose for which information is collected by illion. It was informed illion use de-identified information (this information is not Personal Information as it does not identify any individual/s) for research purposes.	
D.20E.0.6	Div 2, Sec 20G (5), (6) and (7)	N/A	• illion must have policies and processes to ensure that any use or disclosure of credit-related information for the purposes of direct marketing is in accordance with the Privacy Act and the CR Code. • illion must have processes and procedures in place to handle requests from individuals asking the CRB not to use their credit reporting information for direct marketing purposes, and such requests are free to the individual. • illion must have a process to ensure that a written note is made of all uses and disclosures of credit-related information for direct marketing. • illion should have policies and processes to ensure that a register is kept of individuals who have made a request not to receive direct marketing.	Inspected illion's CR Policy and noted that illion does not use or allow credit reporting information to be used for direct marketing as this is not a permissible use. Further, during stakeholder discussion, it was confirmed that illion does not use credit-related information for direct marketing purposes.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
D.20E.0.7	Div 2, Sec 20H, 20J	N/A	• illion must have policies and processes to ensure that pre-screening assessments are only used and disclosed in accordance with the Privacy Act and the CR Code. • illion must have policies and processes to ensure that pre-screening assessments in its control are destroyed once no longer required.	Inspected the Public Access Centre (**PAC**) procedure document and noted the steps to be taken for pre-screening in line with the use and disclosure requirements of the Privacy Act and the CR Code. Inspected the register and noted that records of pre-screening are being maintained.	
D.20E.0.8	Div 2, Sec 20K	N/A	• illion must have policies and processes for receiving and assessing ban requests from individuals. • illion must have policies and procedures to ensure that credit-related information you hold about an individual is not used or disclosed during a ban period. • illion must have policies and processes to ensure that individuals are notified of the end of the ban period, not less than five days before it ends.	Inspected the CR Policy and noted that it covers elements including but not limited to the individual to submit a ban request if they have been a victim of fraud or believe they are likely to be a victim of fraud. Initially, the ban will be in place for 21 days. It also states that: "This will prevent a credit provider from accessing credit reporting information from illion and reduce the likelihood of credit being provided fraudulently. If a ban is put in place illion will confirm with the individual the duration of the ban and inform them when the ban period will expire." Inspected the ban application process and noted that the process incorporates a form and process relating to receiving and assessing ban requests from individuals, controls aiming to ensure that credit-related information you hold about an individual is not used or disclosed during a ban period and to ensure that individuals are notified of the end of the ban period, not less than five days before it ends.	

20K: Protections for victims of fraud

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
D.20K.0.1	Div 2, Sec 20K (1), (2) & (3)	Para 17.1 and 17.3	If illion holds credit reporting information about an individual, it must not use or disclose that information about the individual during the ban period if the individual believes on reasonable grounds that the individual has been, or is likely to be, a victim of fraud (including identity fraud) and the individual requests illion not to use or disclose credit reporting information about them, unless: • the individual expressly consents, in writing, to the use or disclosure of the credit reporting information; or • the use or disclosure of the credit reporting information is required by or under an Australian law or a court/tribunal order. The ban period is the period that starts when the individual makes the ban request and ends either 21 days after the day on which the request is made or on the day after any extension period ends. In relation to an individual ban request illion must immediately: – include on the credit reporting information held in relation to the individual a notation about the individual's request and retain this for the duration of the ban period; and – explain to the individual the effect and duration of the ban period, including that the individual may not be able to access credit during the ban period. Where illion has established a ban	Inspected the CR Policy and noted that individuals are entitled to request a ban on access to their credit file. Inspected the ban application process and noted that once a ban is in place, illion will be prevented from using or disclosing the contents of the individual's credit report during that period, unless required by law or the individual asks illion to use their information. It was noted that the ban period lasted for 21 days from when the ban request was made. It was noted that a notation about the ban would be included on the credit reporting information held in relation to the individual. This notation will be retained for the duration of the ban period. It was also noted courtesy email will be sent to the individual 5 days prior to the end of the ban period ending, indicating when the ban period is due to finish, information on extending the ban period, and contact information. Inspected the ban register and noted that a register is maintained for ban requests that includes (but is not limited to) the date the ban is effective, the BAN expiry date, the date for courtesy notification that ban is about to expire is due to be sent; whether the courtesy notification has been sent and it was noted that the courtesy email was provided 5 business days prior to the end of the ban period.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			period in relation to credit reporting information about an individual, illion must notify the individual not less than 5 business days before the end of the ban period • of the date the ban period is due to finish; • about the individual's rights under Part IIIA, the Regulations and this CR Code to extend the ban period; and • what, if any, information illion requires to support the individual's allegation of fraud.		
D.20K.0.2	N/A	Para 17.2	Where illion receives a request from a CP, mortgage insurer or trade insurer for credit reporting information about an individual in relation to whose credit reporting information a ban period is in effect, illion must inform the CP, mortgage insurer or trade insurer of the ban period and its effect.	During stakeholder discussions, we were informed that the credit reporting information is tagged appropriately for the individual whose ban period is in effect. Inspected two samples of data requests (from the requesting entity to illion) along with the response (from illion to the requesting entity) about an individual in relation to whose credit reporting information a ban period is in effect and noted that the following message, "Consumer Credit file is under ban period" is generated and sent to the requesting entity.	
D.20K.0.3	Div 2, Sec 20K (4) & (5)	N/A	If the individual requests an extension to the ban period (of 21 days) before the period ends, and illion believes on	Inspected the ban application process and noted that the ban period could be extended where the individual requests an extension to the ban period. It was also noted that there was a template relating to notifying the	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			reasonable grounds that the individual has been, or is likely to be, a victim of fraud (including identity fraud) illion must: • extend the ban period by such period as illion considers is reasonable in the circumstances (a ban period for credit reporting information may be extended more than once); and • give the individual written notification of the extension.	individual of the extension to their ban request (either if it was successful or if any information was required).	
D.20K.0.4	Div 2, Sec 20K (6)	N/A	illion must not charge the individual for the making of the request or for giving effect to the request for a ban and/or an extension of a ban period.	Inspected the CR Policy and the ban application process and noted no mention of the fee requirement for requesting a ban and/or extension of a ban period. Further, during stakeholder discussions, it was confirmed that no fee is charged to the individual for making a ban request.	

4.4 Subdivision E – Integrity of credit reporting information

20N: Quality of credit reporting information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
E.20N.0.1	Div 2, Sec 20N	Para 5.4(d), (e) & (f)	illion must take reasonable steps in the circumstances to ensure that the credit information it collects, uses and	Inspected the CCB DQ Procedures in combination with stakeholder discussions and noted that illion undertakes regular testing of the credit information and credit	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			discloses is aligned to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.	reporting information that illion collects, uses and discloses to ensure that it is accurate, up-to-date, complete and relevant, having regard to the purpose for which it is used or disclosed. It was also noted that illion undertakes not only regular testing, but when required, takes steps to initiate targeted testing as applicable, such as where an issue with data quality arises. Further, it was noted that an IT ticket is raised to update the information. Inspected the CCB DQ Procedure, held discussions with DQ stakeholders and noted that the data quality checks are performed across data held by illion from the initial client upload, through usage within the CCB, to deletion if necessary. It was noted that DQ checks, including but not limited to checks for 'default' common names, salacious names, similarities in names, and dummy data are performed on CCB data.	

20Q: Security of credit reporting information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
E.20Q.0.1	Div 2, Sec 20Q (1)	Para 15.1	illion must take reasonable steps in the circumstances to protect the credit reporting information it holds from misuse, interference and loss and unauthorised access, modification or disclosure.	Inspected illion's ASAE 3000 Assurance Report and noted that illion's credit reporting service commitments and system requirements were assessed based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			illion must maintain reasonable practices, procedures and systems to ensure the security of electronic transmission and storage of credit reporting information. illion has the following controls in place: • A process for obtaining and maintaining any relevant information security standards or certifications. • Roles and responsibilities between IT and business users for authorising changes to applications or underlying data are clearly defined, communicated and understood by management and staff. • Staff are advised on how to mitigate against unauthorised access if they discuss customers' or clients' personal information over the telephone. • illion conducts annual information security risk assessments to identify and evaluate security risks, including threats and vulnerabilities the potential impacts of these risks to information (including personal information) handled by an entity. • illion has ICT governance protocols in place. For example, persons responsible for the accreditation and approval of personal information security controls to ensure that each control is effective and appropriate.	100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria) (trust service criteria) and no exceptions were noted. Inspected the illion Risk Management Policy and Framework and noted that it includes the processes for managing risks. Inspected the policy version history and noted it has been reviewed on an annual basis. Inspected the Enterprise Risk Register and noted that it included documentation of IT, Data, Product, and Legal and Regulatory risks. Inspected evidence of one quarterly review performed by the Financial Controller, including communication of the Enterprise Risk Register to Senior Management. Inspected a sample Risk Register Update to the illion Board and noted it contained the risk register and risk management plans. During stakeholder discussions, we were informed that the Companywide Comprehensive Reporting, Privacy, Business Continuity Awareness, and Information Security training courses must be completed by new hires within 14 days of commencement. It was also noted the requirement for team members to complete the training on an annual basis. Further, it was noted that all employees dealing with credit reporting information receive mandatory training, and completion rates are	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			• illion has business continuity and disaster recovery plans that consider information security and breaches. • illion provides information security induction training to employees. • illion provides regular information security refresher training. • illion provides other awareness-raising information (e.g. email newsletters) on information security. • illion staff are made aware of illion's information security policies and procedures. • illion takes reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. • illion has formal and enterprise-wide known policies and procedures in place that specify what to do in case of a (personal) data breach. • illion takes action in order to notify individuals in case of (security) incidents. • illion has a procedure in place to notify the regulator in the event of a data breach. • illion has a procedure in place for media communications in the event of a data breach.	monitored and enforced (including some staff having performance tied directly to training completion). Inspected the screenshot which details training material which is required as part of illion's 'Annual Compliance Training AU 2021' and noted the compulsory trainings were titled, 'Anti-bribery and conflict of interest'; 'Equal employment opportunity'; 'Policy review'; 'Privacy AU'; 'Workplace health and safety'; and 'email security'. It was noted all these trainings were marked as mandatory. Inspected a sample user's training program and noted that Privacy, Compliance, Email Security, Anti-bribery training, etc., were included as mandatory. Inspected the illion Business Continuity policy and noted that it outlined the requirements to identify and respond to disruptions, including the key roles and responsibilities involved in resuming business operations. Inspected a sample Business Continuity Plan Test performed during the year and noted that the test passed. Inspected the illion Access Management Policy and noted that it includes minimum requirements for passphrases to access the illion network, applications, and databases. Inspected approval artefacts for a user who was granted access to the Consumer Credit Bureau database and noted that the request was approved prior to provisioning.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			• illion records incidents in a formal incidents log and actions documented and tracked for remediation. • illion conducts a root cause analysis of incidents that occur.	Inspected a sample of the user whose access to the Consumer Credit Bureau database was terminated and noted that access was terminated on the date of termination. Inspected monthly Mercantile User Access Review documents and noted that User Access Review was completed on time and appropriate actions were taken. Inspected approval artefacts for a user who was granted remote access and noted that the request was approved prior to provisioning. Inspected the illion IT Change Management Policy and noted that it includes change types, approval levels, and roles and responsibilities. Inspected a sample of normal system change and noted that Change Advisory Board (**CAB**), Testing, and Business Owner approvals were in place prior to implementation. Inspected the illion Policy Backup and Recovery and noted it outlines the requirements for backup, including retention periods, schedules, and reporting. Inspected a sample of server backup history and noted that the backup was completed. Inspected the Vulnerability Management Policy and noted that it includes vulnerability assessment processes,	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
				including the frequency, severity categorisation, escalation procedures, remediation strategies, and reporting. Further, CCB Security Assessment was carried out by an independent third party in September 2020, and for a sample of findings, it was noted that the finding was tracked to closure. Inspected the Privacy Policy and noted that it outlines illion's privacy policy and data protection practices relating to Risk & Marketing Solutions. Inspected the Privacy Breach Response Plan and noted it outlines the process to assess, investigate, notify of privacy breaches, and rectify privacy breach issues. Inspected Privacy Breach Register and noted that the suspected breaches and required actions were adequately recorded.	
E.20Q.0.2	Div 2, Sec 20Q (1) & (3)	N/A	illion must take reasonable steps in the circumstances to protect the credit reporting information it holds from misuse, interference and loss and unauthorised access, modification or disclosure. illion must maintain reasonable practices, procedures and systems to ensure the security of electronic transmission and storage of credit reporting information. illion must store the credit reporting information it holds:	During stakeholder discussions, we were informed that data on the backup servers, SAN storage, production servers, and laptop is encrypted. Further, no USB device is permitted to connect to the illion systems. Inspected sample artefacts and noted that the data is encrypted on the backup server, SAN storage, production server, and laptop. Inspected illion workstation production security settings and noted whitelisted applications were identified. Further,	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			a) either: (i) in Australia or an external Territory; or (ii) in accordance with any security requirements prescribed by the regulations for storing the information outside of Australia and the external Territories; and b) in accordance with any security requirements prescribed by the regulations. illion has the following technical security controls in place: • Encryption of data at rest (e.g. in databases or on cloud storage) • Encryption of data in transit (e.g. over the internet) • Encryption of backups • Encryption of portable storage devices (e.g. USB storage devices) • Encryption of workstations (e.g. employee laptops) • Processes for managing (e.g. revoking) cryptographic keys • Application whitelisting • Application blacklisting	we were informed that illion blocks all the applications by default unless approved and whitelisted. Inspected CCB high-level network diagram and noted that a demilitarized zone is identified. Further, perimeter and internal firewall are placed to protect the network. Inspected security architecture diagram and noted that firewalls are implemented to detect and prevent network-based anomalies. Further, a Security Information and Event Management (**SIEM**) solution and network Data Loss Prevention (**DLP**) is implemented to monitor security incidents. Inspected laptop baseline security settings and noted that machine lockout configuration is set to 900 seconds of inactivity. Inspected domain password policy and noted appropriate password parameters are configured. Inspected consumer profile security requirements and noted that Multi-Factor Authentication (**MFA**) is enabled. Inspected illion remote access procedure and noted that the registry key is to be checked on each illion machine for remote access. Inspected a sample user machine's security settings and noted that Universal Serial Bus (**USB**) is disabled.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			• Firewall and DMZs • Malware, Intrusion and Detection controls • Users should be advised to lock their computers when they leave their desks, even for short periods. • Computers should be configured to automatically lock after a set time. • illion has enforced rules around passwords (e.g. password complexity, a password history policy). • illion has two-factor authentication. • illion has additional controls (e.g. use of a VPN) for remote access to personal information. • illion has systems in place to monitor and detect unauthorised downloading, transferring or theft of bulk data, for example through the use of personal storage devices. • illion has restricted access areas controlled and managed (specifically for the facilities housing systems storing/processing Personal Information and communications equipment controlling its transfer).	Inspected the illion Policy Physical Security and noted it outlines the requirements including but not limited to premises area, reception and visitor protocol, physical entry controls, computer and communication equipment security, accessing protected classified information. Inspected sample artefacts and noted physical security controls are implemented at illion.	
E.20Q.0.3	Div 2, Sec 20Q (1)	N/A	illion must take reasonable steps in the circumstances to protect the credit reporting information it holds from	Inspected illion Policy Mobile Devices and noted that illion has controls in place around mobile devices including BYOD which are applicable to all illion employees, consultants, vendors, contractors and others using a	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			misuse, interference and loss and unauthorised access, modification or disclosure. illion must maintain reasonable practices, procedures and systems to ensure the security of electronic transmission and storage of credit reporting information. illion has the following controls in place around mobile devices (including BYOD) of employees and contractors, such as: • enforced access controls (e.g. phone unlock code) • encryption of data on device • remote wipe • segregation of work and personal data • additional training/policies relating to remote work	business or private mobile handheld device on any premises occupied by illion. It was noted that controls include a requirement for the device to be configured with encryption software and/or hardware that encrypts the entire hard disk, a compliant passcode lock that requires a user to authenticate before the system may be accessed, devices may be remotely wiped by illion (including privately owned BYOD devices), there is a requirement to segregate illion information from personal or non-illion information (segregate work and personal data), and there is an additional policy dedicated to remote access.	
E.20Q.0.4	Div 2, Sec 20Q (1)	N/A	illion must take reasonable steps in the circumstances to protect the credit reporting information it holds from misuse, interference and loss and unauthorised access, modification or disclosure. illion must maintain reasonable practices, procedures and systems to ensure the security of electronic transmission and storage of credit reporting information.	Inspected illion Policy Third Party Management v4.5 and noted illion has controls in place around third parties. It was noted in particular that a vendor risk assessment is conducted for all third parties by way of a third party supplier security questionnaire which is also to ensure that controls are implemented by third parties to ensure confidentiality, integrity and availability of illion information, in accordance with illion's Information Security Policy. It was noted that it is a requirement that all service levels agreed with third parties are monitored on a period basis	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			illion has the following controls in place around third parties: • illion conducts security and privacy risk assessments of third parties (e.g. cloud providers, vendors). • illion has controls in place (e.g. contractual clauses) to ensure that third parties provide appropriate privacy and security protections. • illion has processes in place to monitor privacy incidents (breaches, enquiries or complaints) relating to personal information handled by third parties. • illion undertakes periodic reviews (e.g. external audits) of third parties' privacy and security controls. • illion reports the results of third party monitoring and assurance regularly to management.	(period must be specified in contract) to ensure that all terms in the contract are being adhered to. It was also noted in relation to data breaches or suspected security incidents that the following controls are in place: 1) regular meetings with third parties to discuss service level reviews and any potential security incidents that relate to services provided by that third party; 2) when a data breach has been identified there is a requirement for third parties to alert their main illion contact and determine next steps; 3) all cyber security incidents should be reported to the organisation's Chief Information Security Officer (**CISO**). Inspected illion's procurement procedure and noted that vendor monitoring will require either: a) yearly monitoring where the vendor participates in yearly meetings with procurement and key stakeholders; or b) formal quarterly monitoring where the vendor will be required to participate in the illion vendor management program. It was also noted that annual information security will be conducted including the following: 1) onsite information security (illion to conduct an on-site audit of the vendor's premises where illion data is held, in order to identify areas of concern and provide rectification recommendations in those areas); 2) annual audit of vendor policies (vendor to provide all relevant policies regarding data collection, storage,	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
				usage, transmission, and privacy act (such as PII)); and 3) annual vendor contract audit (procurement/legal to review current contract and make recommendations for any variations). Inspected third party assessment reports and noted that areas including, but not limited to, information security policies, access control, cryptography, compliance, supplier relationships and physical and environmental security, were assessed.	
E.20Q.0.5	Div 2, Sec 20Q (1)	N/A	illion must take reasonable steps in the circumstances to protect the credit reporting information it holds from misuse, interference and loss and unauthorised access, modification or disclosure. illion must maintain reasonable practices, procedures and systems to ensure the security of electronic transmission and storage of credit reporting information. illion has the following controls in place around physical document security: • a 'clean desk' policy. • procedures governing the printing of documents containing personal information.	Inspected the Physical Security Policy and noted controls in place around physical document security. It was noted that all visitors and team members must display their illion provided identification (i.e. illion issued access cards) at all times within an illion occupied facility. Inspected the Acceptable Use Policy and noted physical security controls in the form of requirements that all illion staff and contractors must follow. This included the requirement for all devices to be physically secured, the requirement to maintain a clear desk and clear screen requirement, meaning that desks must be free of any paper copies of illion information classified as 'confidential' or 'internal use' and such physical copies should be physically secured when not a requirement and especially at the end of the work day when vacating the office. There is also a requirement that printing classified as 'confidential' or 'internal use' must be immediately	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			• physical security controls (e.g. access cards) in place to prevent unauthorised access to premises and systems.	collected from printers and fax machines. It was also noted that illion staff and contractors cannot grant access to anyone who is not authorised to be in the area or lend access passes.	
Credit Provider contracts, audit and breaches					

E.20Q.0.6	Div 2, Sec 20N (3) and 20Q (2)	Para 2.1 and 15	illion must enter into written agreements with CPs that require the providers to:
			• ensure that credit information that they disclose to illion is accurate, up-to-date and complete
			• protect credit reporting information that is disclosed to them from:
			  • misuse, interference and loss; and
			  • unauthorised access, modification, or disclosure.
			The agreement illion enters into with a CP must also oblige both parties to comply, to the extent applicable from time to time, with Part IIIA, the Regulations and the CR Code.
				Inspected two sample master service agreements (between illion and CBA and illion and Westpac) and noted that agreements included clauses requiring data to be protected from misuse, interference, and loss and from unauthorised access, modification, and disclosure. It was also noted clauses requiring providers to ensure the information that they disclose to illion is accurate, up-to-date, and complete.	

E.20Q.0.7	N/A	Para 23.1 & 23.2	To ensure illion is able to tailor the frequency and extent of any audit requirements under Part IIIA to the CPs that present the greatest risk of non-compliance, it must establish a documented, risk based program to monitor CP's compliance with their obligations under Part IIIA incorporated in their agreements with illion which must:	Inspected illion's Risk Based Monitoring Program and noted that illion establishes a documented, risk-based program to monitor CPs' compliance with their obligations under Part IIIA, which is incorporated into the written agreements, and ensures that illion is able to tailor the frequency and extent of audits based on the level of risk of	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status

			• identify and evaluate indications of risk of non-compliance by CPs with their obligations to:
			  • disclose credit information that is accurate, up-to-date and complete to illion;
			  • protect the credit reporting information that illion discloses to the CP from misuse, interference and loss and from unauthorised access, modification or disclosure; and
			  • take the steps in relation to correct credit-related personal information required by Part IIIA, the Regulations and the CR code
			• assess the risk posed by CPs of significant non-compliance with those obligations utilising those risk indicators and the range of information available to illion including correction requests and complaints
			• utilise a reasonable range of monitoring techniques to validate and update those risk assessments from time to time
			• include an audit program for CPs to assess compliance with their obligations referred to in paragraph 23.1 of the CR code.
				non-compliance for each CP. It was also noted that illion's risk-based program contains all the requirements listed in the Summary of Obligations. The following criteria are established to determine high-risk audit areas:
				1) New to illion;
				2) New to the industry;
				3) New data sets (i.e the entity changes products/services/level of data exchange);
				4) Correction volumes. illion recognises correction requests as being an indicator of potential issues (correction requests irrespective of how they are made, whether by the consumer, their representative or the customer themselves);
				5) Systemic issues (illion becomes aware of a systemic issue, and notes this is strong indicator of risk);
				6) Individual data point volumes (excessive use of a particular data point may also be an indicator of increased risk);
				7) Complaint volumes; and
				8) Uniqueness (unique product offering, method of service provision or use case).
				The above eight risk indicators also have corresponding strength indicators and actions associated. For example, the number of complaints is considered a medium strength indicator, and actions include 'Consider if action could impact other consumers. Consider other Risk criteria'.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
E.20Q.0.8	Div 2, Sec 20N (3)(b) & (c) and 20Q (2)(b) & (c)	Para 23.1, 23.3, 23.4, 23.5 & 23.6	illion must: • ensure that regular audits are conducted by an independent person to determine whether agreements entered into with CPs are being complied with; and, • identify and deal with suspected breaches of those agreements. illion's risk based program must include a CP audit program for CPs to assess compliance with their obligations to ensure that: • credit information the CP discloses to illion is accurate, up-to-date and complete; • credit reporting information illion discloses to the CP is protected from misuse, interference, loss, and from unauthorised access, modification or disclosure; and • the CP takes steps in relation to requests to correct credit-related personal information required by Part IIIA of the Act, the CR Code and the Regulations. To be independent to conduct an audit of a CP as part of illion's auditing program, an auditor: • must not be a director or employee of the CP, have a significant financial interest in the CP or, at any time	It was noted that illion's Risk Based Monitoring Program states that it operates accordance with independence requirements under Part IIIA of the Privacy Act (as set out in the Summary of Obligations). During stakeholder discussions, we were informed that illion's Privacy Compliance Officer conducts the audits as part of the CP audit program, and reports to the Chief Legal Officer, whom reports to the Chief Finance Officer. Inspected the CP example walkthrough document and noted that 13 CPs were assessed as having Serious Credit Infringements (**SCI**s) in November and December 2020. It was noted that an information request was made to the CP, data was sent to the CP to allow them to review individual records, a request was sent for appropriate supporting documentation from the CP, instructions then sent from the CP to remove SCIs.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			during the previous 12 months, had any such relationship or interest; • must achieve functional independence of illion's organisational structure and supervision arrangements if the auditor is an employee of illion or functional independence of an organisation's governance and supervision arrangements if an employee of an industry funded organisation; and • must not have any other association that would impair the perception of the auditor's independence, nor had any such association at any time during the previous 12 months. illion must take reasonable steps to ensure that a person who conducts an audit of a CP as part of its auditing program has sufficient expertise for the role including knowledge of Part IIIA of the Act, the CR Code and the Regulations, audit methodology and previous experience in conducting audits and credit reporting system experience. illion must take reasonable steps to ensure that its audit oversight, including reporting arrangements, is sufficient to enable it to form a view as to whether the CP is complying with its obligations.		
E.20Q.0.9	N/A	Para 5.4(g)	Where illion identifies credit information that is not accurate, up-to-date and complete, raise this, where	Inspected CCB Batch Technical Documentation and Consumer Credit Data flow diagram and noted that default	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			reasonable, with the CP that disclosed the information and request the CP to: • take reasonable steps to review its credit information management practices, procedures and systems; • rectify any issues that are identified; • advise illion of the results of the review; and • illion must have reasonable practices, procedures and systems that are designed to cover its legislative obligations and enable it to report about its testing (undertaken in accordance with paragraph 5.4(d) of the CR code), and any material findings or material changes to procedures, to CPs with which it has an agreement with in relation to the disclosure of credit information (by the CP) to illion and disclosure of credit reporting information (to the CP) by illion as referred to in section 20N(3) and section 20Q(2) respectively.	data loading process is formally documented. The process involves the following steps: 1) Client will build a batch default update file; 2) The batch file is then dropped into illion's SFTP server location folder; 3) The batch file is picked up by illion for processing through an automated program; 4) The batch file is processed overnight, and three Response files are generated: i) Log file (This file contains the general attribute of the file. For example: No. or records in the file, No. of records successfully processed, etc.); ii) Response file (This file contains file header, consumer header, customer transaction header, individual details, and file trailer details); iii) Error file (This file contains information about the number of records and associated error messages because of any technical issue or data that was not agreed with CPs). 5) The above-mentioned batch response files are then placed in the illion's SFTP server response folder; 6) The batch files are then placed in the CPs SFTP server location folder; and 7) The batch files are then picked up by CPs to perform suitable action. Inspected the CCB DQ procedures and noted that there are practices and processes in place to locate issues or errors associated with information disclosed to illion by	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
				CPs. This includes DQ clean-ups such as DOB, similar names, salacious names, in order to populate customer files with correct and required information.	
Credit reporting system integrity					
E.20Q.0.10	N/A	Para 23.11	illion must publish on its website by 31 August each year a report for the financial year ending 30 June of the same year that includes information about the following: • Access • Corrections • Complaints • Serious credit infringements • illion's monitoring and auditing activity • Disclosure of CCLI and RHI to illion • Any other information requested by the Commissioner.	Inspected illion's website and confirmed that the report was published on the website, dated August 2020. Inspected the report and noted that it includes information covering access, corrections, complaints, serious credit infringements, monitoring and auditing activities, and disclosure of CCLI and RHI to illion.	

4.5 Subdivision F – Access to and correction of information

20R: Access to credit reporting information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
F.20R.0.1	Div 2, Sec 20R (1), (2) & (3)	Para 19.1 & 19.2	If illion holds credit reporting information about an individual, illion must, on request by an access seeker, grant that access seeker access to the information. illion must respond to a request for access within 10 days. However, it must not grant access without first obtaining reasonable evidence necessary to satisfy itself as to the identity of the person making the request and their entitlement to access under relevant privacy laws. These policies and procedures should ensure that access is provided free once every 3 months, or if an individual has been refused credit in the previous 90 days. illion should have prominent information advising individuals of their right to obtain credit-related information free of charge.	Inspected the CR Policy and Privacy Policy and noted it includes a section outlining how an individual can access their credit reporting information held by illion, including contact details and a link to the website that users can access to get their credit information. Also noted that it states credit information will only be provided subject to the individual being appropriately identified first. Inspected the illion website and noted that it states, '*See your credit score and credit report for free*'. Inspected the Manual ID Verification Process and noted that individuals could only access score and report information once the verification checks are completed. Inspected the PAC Process Flows (Manual Application Process) and noted that verification checks and matching the customer to the correct Bureau file are key parts of the process before releasing the report to the customer. During stakeholder discussions, we were informed that manual ID verification has a one-day turnaround time (i.e., verifications that are not completed using the dedicated access website). It was also noted that this online platform allows unlimited access to an individual. There are no charges for access, irrespective of how often an individual may choose to access their report. Further, we were informed during the discussions that when an	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
				individual request a manual report through the PAC team, no fee is charged to the individual. Inspected the Application Register in conjunction with stakeholder discussions and noted that the Application Register includes the date of the request and the date of providing access for manual verifications. On inspection of the Application Register extract provided of 100 samples, it was noted that all manual requests were responded to in 10 working days or less.	
F.20R.0.2	Div 2, Sec 20R (4)	Para 19.4 & 19.6	For access free of charge, illion must provide the access seeker with access to: • all credit information relating to the individual currently held in the databases that illion utilises for the purposes of making disclosures permitted under Part IIIA; and • all current illion-derived information about the individual that is available, presented clearly and accessibly with reasonable explanation and summaries of the information to assist the access seeker to understand the impact of their credit worthiness. if not provided in the manner requested by the access seeker, then illion must take reasonable steps to provide access in a way that meets the needs of illion and the individual.	Inspected the CR Policy and Privacy Policy and noted it includes a section outlining how an individual can access their credit reporting information that is held by illion, including contact details, and a link to a part of the website which users have the option to use to get their credit information. Also noted that it states credit information will only be provided subject to the individual being appropriately identified first. Inspected the illion website and noted that it states, 'See your credit score and credit report for free'. Inspected the PAC Access Request Register and noted the register listed 17 access requests that have been granted, with access request dates between 1-9 June 2021.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			Where illion derived information about the individual is provided to an access seeker, illion may do so in a way that preserves the confidentiality of the methodology, data analysis methods, computer programs or other information that is used to produce the derived information.		
F.20R.0.3	Div 2, Sec 20R (2) & (7)	N/A	illion is not required to give an access seeker access to credit reporting information if: • giving the access would be unlawful; or • denying access is required or authorised by or under an Australian law or a court / tribunal order; or • giving access would be likely to prejudice one or more enforcement related activities conducted by or on behalf of an enforcement body. Where illion refuses to give access to information based on one of the reasons above, illion must give a written notice to the assess seeker that: • sets out the reasons for the refusal unless it is unreasonable to do so; and • states that if the access seeker is not satisfied with the response to the request, the access seeker may access the recognised EDR scheme which illion is a member of or make a complaint to the Commissioner under Part V of the Privacy Act.	Inspected the PAC Access Request Register and noted that all the requests processed have listed 'documents provided' are lawful document types. During stakeholder discussions, we were informed that there are only three reasons illion will deny access, including where no data is held about the individual, where there is inadequate identification, or where the automated verification is referred back to illion Credit Check (**iCC**) for manual verification (in this case, access will be provided if ID checks can be completed manually). Inspected six example emails of instances where a customer had been denied access and noted that illion sets out reasons for refusal.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
F.20R.0.4	Div 2, Sec 20R (6)	Para 19.3	If a request has been made within the previous 3 months, illion may charge the access seeker for giving access to the information, but not for making the request and the charge must not be excessive. Where illion has a fee-based service for providing an access seeker with credit reporting information: • the information it makes available about the fee-based service must prominently state that individuals have a right under Part IIIA to obtain their credit reporting information free of charge in the following circumstances: – if the access request relates to a credit provider's decision to refuse the individual's consumer credit application – if the access request relates to a decision by a credit reporting body or credit provider to correct credit reporting information or credit eligibility information about the individual; and – once every 3 months • illion must take reasonable steps to ensure that its service, whereby individuals may obtain their credit reporting information free of charge, is as available and easy to identify and access as its fee-based service.	During stakeholder discussions, we were informed that illion does not have any fee-based services for providing access to credit reporting information.	

20S: Correction of credit reporting information

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
F.20S.0.1	Div 2, Sec 20S (1), 20T (2), (3) & (4) and 20U	Para 20.4	Upon request by an individual, and if illion is satisfied that the credit-related personal information it holds about that individual is inaccurate, out-of-date, incomplete, irrelevant or misleading, illion must, within 30 days from when the request to correct was made or a longer period which the individual has agreed to in writing, take reasonable steps (if any) in the circumstances to: • correct the information • ensure that any future derived information is based on the corrected credit information • ensure that any derived information that is based on the uncorrected credit information is not disclosed or used for the purpose of assessing the credit worthiness of the individual to whom the information relates. If it considers that it cannot satisfy itself that the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, illion must consult with another CRB and / or CP which has an Australian link and holds or held the information.	Inspected the CR Policy and Privacy Policy and noted that the same website that is used to access credit information is also used for correction requests, and this website is clearly made available to customers in both the CR Policy and the Privacy Policy several times. Inspected the PAC Procedure and noted a requirement for PAC consultants to take actions where a request is received from an individual for an amendment to their credit report, including: 1) Update Form or Query Request correspondence is date stamped and recorded into the PAC Amendment Register. 2) Place a note of the queried entry on the credit report until the matter is resolved. The note is to be inserted within 5 working days. 3) If it is established that an amendment is required to the credit report this amend must take place within 5 working days. 4) Advise of the outcome to the individual where an amendment has been made, within 14 days of having made the amendment. 5) Derived information that is based on the uncorrected credit information is not disclosed or used for the purpose of assessing the credit worthiness of the individual to whom the information relates. If the individual's consumer credit information has been accessed by an enquiring credit provider during the	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
				previous 3 months of the correction date, it was noted that illion will notify the nominated persons of the changes. 5a) Similarly, where the individual advises illion that another person has been given information from their credit report, illion will notify those persons of the changes. Inspected the correction request logs and noted that illion records personal information update requests, queries and disputes in a register.	
F.20S.0.2	N/A	Para 20.2 (a)	If consulted by another CRB or CP about a correction request, illion must take reasonable steps to respond to the consultation request as soon as practicable.	Inspected the Corrections Process for CP requests and noted an appropriate process for corrections requested, including broad areas of enquiry removals, default removals and updates, RHI removals and updates, and CCLI removals and updates (non-exhaustive list). The process includes sending a response to the correction request. During stakeholder discussions, we were informed that CRB correction requests are conducted in the same way as noted in the Corrections Process for CP requests.	
F.20S.0.3	N/A	Para 20.3	If illion forms the view that it will not be able to resolve an individual's correction request within the 30 day period, illion must as soon as practicable:	Inspected the PAC Procedure and noted a requirement for PAC consultants to take actions where a request is received from an individual for an amendment to their credit report, including:	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			• notify the individual of the delay, the reasons for this and the expected timeframe to resolve the matter • seek the individual's agreement to an extension for a period that is reasonable in the circumstances • advise that the individual may complain to a recognised EDR scheme which illion is a member of (and provide contact details for that scheme) or to the Commissioner. If the individual has not agreed to the requested extension, illion must as soon as practicable provide a response to the correction request within the timeframe sought for extension.	1) Update Form or Query Request correspondence is date stamped and recorded into the PAC Amendment Register. 2) Place a note of the queried entry on the credit report until the matter is resolved. The note is to be inserted within 5 working days. 3) If it is established that an amendment is required to the credit report this amend must take place within 5 working days. 4) If illion forms the view that it will not be able to resolve an individual's correction request within the 30-day period, the procedure requires illion to contact the individual in relation to the delay. Inspected the correction request logs and noted that illion records personal information update requests, queries and disputes in a register. Inspected the PAC process flow and noted that it does not include timeframes. Inspected steering committee slides and noted that correction request timeframes are monitored, and it was noted that in March 2021 the average time for a correction to be finalised was 7 days, February was 8 days, and January was 9 days. Inspected two sample notices provided to the individual and noted that illion provides a date in which it expects to have the complaint resolved by, but it does not seek the individual's agreement to an extension nor does it advise	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
				that the individual may complain to a recognised EDR scheme which illion is a member of or the Commissioner.	
F.20S.0.4	N/A	Para 20.5 & 20.6	If, under paragraph 20.5(a), illion is satisfied that default information is inaccurate, out-of-date, incomplete, irrelevant or misleading, having regard to the purpose for which the information is held by illion then illion must correct the credit reporting information by destroying that default information.	During stakeholder discussions, it was noted that Consumer Credit Bureau (**CCB**) database records that are due for deletion are staged for 30 days and then deleted. Physical records are destroyed, and destruction confirmation certificates are provided. Inspected the CCB DQ procedures and noted that a number of automated clean up activities such as dummy DOB deletion, duplicate default deletion, and duplicate directorship deletion are scheduled for CCB database. Inspected the document having information of the records removed from CCB for Jan, Feb and March 2021, and noted that it contains the number of records which were archived and the number of records that were deleted from the CCB database, by 'information type' (e.g. bankruptcies deleted, accounts deleted, accesses deleted, etc) and by date.	
F.20S.0.5	Div 2, Sections 20S (2) & (3) and 20U (2), (4) & (5)	Para 20.7	If, on request by an individual, illion makes a correction to credit-related personal information, illion must give the written notice of correction to the following within 5 business days of the decision: • The individual the correction relates to	Inspected the PAC Procedure and noted a requirement for PAC consultants to take actions where a request is received from an individual for an amendment to their credit report, including: 1) Update Form or Query Request correspondence is date stamped and recorded into the PAC Amendment Register.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			• The interested party, i.e. the CP or CRB it consulted with (if applicable) regarding a correction request • The recipient of the information if illion had previously disclosed the information (apart from disclosures made for the purposes of determining whether unsolicited credit information could have been collected by illion if it had solicited the information, or for purposes of consulting with another CRB or CP regarding a correction request) unless it is impracticable for illion or illion is required by or under an Australian law or a court / tribunal order not to give the notice.	2) Place a note of the queried entry on the credit report until the matter is resolved. The note is to be inserted within 5 working days. 3) If it is established that an amendment is required to the credit report, this amendment must take place within 5 working days. 4) Advise of the outcome to the individual where an amendment has been made, however it is noted that the timeframe for this outcome notification was 14 days. It is noted that this has since been updated in the PAC Procedure in line with the obligation to advise of the outcome to the individual within 5 days of making the amendment. *Note: At the time of our testing, the correction notification timeframe to the individual was not aligned to obligations in illion's process document. The process document has now been updated, and the correction notification timeframe to the individual is now aligned to obligations.*	
F.20S.0.6	Div 2, Sections 20 S (2), 20U (2)	Para 20.7 & 20.9	The notice to the individual must: • explain what CRBs, CPs and affected information recipients (**AIR**) illion is intending to notify (only applicable if illion relies on paragraph 20.9 of the CR Code) • ask the individual if there is any other CP or affected information recipients that the individual would like	Inspected the PAC Procedure and noted a requirement for PAC consultants to take actions where a request is received from an individual for an amendment to their credit report, including: 1) Provide a copy of amended credit information to allow an individual to check the information 2) Ask the individual if there is any other CP or affected information recipients that the individual would like illion to notify	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			illion to notify (only applicable if illion relies on paragraph 20.9 of the CR Code) • include all relevant credit reporting information held by illion so that the individual can check that the information has been appropriately corrected • explain that the individual has a right under the CR Code to obtain their credit reporting information from illion free of charge if the access request relates to the decision by a CRB or a CP to correct information about the individual, and how that right may be exercised. Unless it is impracticable or illegal to do so, the notification obligation is met if within 7 business days of the correction illion gives notice of the correction to: • All CRBs to which it disclosed the pre-corrected information; • All CPs and affected information recipients to which it disclosed the pre-corrected information within the previous 3 months; and • Any other CP or AIR nominated by the individual and to which it disclosed the pre-corrected information more than 3 months previously.	3) Notify the CRB, CP or the AIR of the correction within 30 days. However, it is noted that the timeframe was updated to 7 business days in line with the obligations. 3a) illion will notify CPs who have accessed the individual's credit information in the 3 months prior to the correction being made. 3b) Any person the individual nominates who has been given information from their credit report will be contacted and notified of the changes due to the correction. Inspected two example emails and noted that illion provides customers with an email notification detailing which CRBs, CPs and affected information recipients illion has notified within 7 business days of the correction. *Note: At the time of our testing, the correction notification timeframe to the CRBs, CPs, or AIR was not aligned to obligations in the illion's process document. The process document has now been updated, and the correction notification timeframe to the CRBs, CPs, or AIR is now aligned to obligations.*	
F.20S.0.7	N/A	Para 20.9	Only applicable if illion relies on paragraph 20.9 of the CR Code: Unless it is impracticable or illegal to do so, if notice is given to a CP or AIR that previously received illion	Inspected PAC Procedure and noted that PAC consultants are required to notify enquiring credit providers or other	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			derived information that is no longer correct by reason of the correction, the notice must include revised illion derived information that has been derived using the correct information.	parties nominated by the individual of the changes to the individual's consumer credit information.	
F.20S.0.8	N/A	Para 20.8	Where illion corrects credit-related personal information by updating identification information about an individual, illion is not obliged to notify any previous recipient of the information about the updating of that information, unless requested by the individual.	Inspected the PAC Procedure and noted a requirement for PAC consultants to take actions where a request is received from an individual for an amendment to their credit report, including to notify any person the individual nominates whom has been given information from their credit report will be contacted and notified of the changes due to the correction.	
F.20S.0.9	Div 2, Sec 20T (5)	N/A	illion must not charge the individual for requesting the correction or for correcting the information.	During stakeholder discussions, we were informed that the individual is not charged for requesting the correction or for correcting the information.	
F.20S.0.10	Div 2, Sec 20U (3)	N/A	If illion does not correct the personal information in response to an individual request, illion must give the individual written notice which covers the following within a reasonable period: • states that the correction has not been made • sets out illion's reasons for not correcting the information, including evidence substantiating the correctness of the information	Inspected the PAC Procedure and noted that if illion does not correct the personal information in response to an individual request, the process states that PAC consultants are required to give a notice that states the correction has not been made and the reasons why, and must state the individual's right to complain to the Privacy Commissioner. Inspected two sample emails which are sent to individuals when illion was not able to correct the personal information in response to an individual's request and noted that the emails states why the correction was not	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			• states that if the individual is not satisfied with the response to the request, the individual may access the recognised EDR scheme which illion is a member of or make a complaint to the Commissioner.	made, sets out reasons for not correcting the information, and states that if the individual is not satisfied with the response there is a link to the complaints website at illion, and it is noted that complaints may also be made to AFCA or its relevant EDR scheme.	

23B: Dealing with complaints

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
F.23B.0.1	Div 5, Sec 23B (1) and 23C (2)	Para 21.3 & 21.5	If a complaint is made to illion about its acts or practices that may be a breach of certain provisions of Part IIIA or the CR Code, illion must investigate the complaint and make a decision about the complaint. Specifically, illion must: • give the individual a written notice within 7 days after the complaint is made that acknowledges the making of the complaint and sets out how illion will deal with the complaint • investigate the complaint • give the individual a written notice that sets out the decision and states that if the individual is not satisfied with the decision, the individual may access a recognised external dispute resolution (EDR) scheme	Inspected the internal Complaints Handling Procedure and noted illion investigates and makes decisions about complaints. It is noted that once illion receives a complaint, it will assign a complaint handling officer who will then acknowledge the complaint within 5 working days and respond with written advice as soon as possible thereafter, generally within 30 days.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			of which illion is a member of or make a complaint to the Commissioner within 30 days from the day the complaint was made or a longer period that the individual has agreed to in writing. illion must consult a CRB or CP about the complaint if it considers it necessary, and the use or disclosure of personal information for this purpose is permitted under the Act. If illion is consulted by another CRB or CP about a complaint, illion must take reasonable steps to respond to the consultation request as soon as practicable. If the complaint relates to credit information or credit eligibility information that a CP holds, illion must notify the provider of the making of the complaint and the making of a decision about the complaint as soon as practicable after each are made unless it is impracticable to give the notification or illion is required by or under an Australian law, or a court / tribunal order, not to give the notification. Unless it is impracticable or illegal to give notice to a CP about a complaint relating to a CRB's act of practice that may breach Section 20S, this obligation is taken to be met if illion gives notice as soon as practicable to: • the CP if the complaint relates to credit information that was disclosed to illion by a CP • any other CP to which illion disclosed the credit information to which the complaints relates in the previous 3 months		

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			• any other CP that has been nominated by the individual for this purpose.		
F.23B.0.2	N/A	Para 21.4	If illion forms the view that it will not be able to resolve a complaint within the 30 day period required by Part IIIA, illion must: • inform the individual of this before the end of the 30 day period and provide the reason for the delay, the expected timeframe to resolve the complaint and seek their agreement to an extension for a period that is reasonable in the circumstances • advise that the individual may complain to the recognised EDR scheme of which illion is a member, and provide the contact details for that scheme, or to the Commissioner.	Inspected the internal Complaints Handling Procedure and noted illion will take steps to advise the complainants if illion requires more than 30 days (to obtain additional information relating to the complaint) and seek the complainant's agreement to an extension for a period that is reasonable in the circumstances. It was also noted that illion includes on its complaints handling procedure (published online and available to consumers) that consumers may also refer their matter to AFCA (the recognised EDR scheme of which illion is a member), and provides the contact details for that scheme, as well as details of the OAIC. Inspected the internal Complaints Handling Procedure and noted that it reflected the 30 day timeframe requirement for responding to complaints, with a requirement for written consent from the complainant if the 30 day timeframe needs to be extended. It was also noted that there was a link to a template used for the extension of time request, and the written consent must include: • inform the individual of this before the end of the 30-day period; • provide the reason for the delay; • provide the expected timeframe to resolve the complaint;	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
				• seek their agreement to an extension for a period that is reasonable in the circumstances; and • advise that the person may complain to the recognised external dispute resolution scheme	
F.23B.0.3	Div 5, Sec 23C (4)	N/A	If illion discloses credit reporting information to which the complaint relates and a decision has not been made about the complaint at the time of the disclosure, illion must notify in writing the recipient of the information of the complaint at that time unless it is impracticable to give the notification or illion is required by or under an Australian law, or a court / tribunal order, not to give the notification.	Inspected screenshot of illion credit check configuration settings, held stakeholder consultations, and noted that credit checks are flagged as 'investigating', when the entry is referred as a query or dispute and is retained in the 'investigating' status until resolved. Inspected the register containing credit disclosures, held discussions with stakeholders and noted that the record is a tagged as "Has Dispute" and the recipient is returned with information stating that there is a dispute relating to the information.	
F.23B.0.4	Div 5, Sec 23A (5)	N/A	illion must not charge the individual for making of the complaint or for dealing with the complaint.	Inspected the internal Complaints Handling Procedure and noted that illion would not charge a complainant to make a complaint.	
F.23B.0.5	N/A	Para 21.2	illion must be a member of a recognised EDR scheme.	Inspected illion's certificate of membership with the Australian Financial Complaints Authority Limited and noted current membership is valid until 31 July 2022.	
F.23B.0.6	Div 2 Sec20B 2(b)	N/A	illion must have documented policies, processes and procedures in place for receiving and dealing with privacy inquiries or complaints from individuals.	Inspected the internal Complaints Handling Procedure and noted that this is a procedure for receiving and dealing with individual privacy inquiries or complaints. This	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			illion has a complaints process complying with relevant industry codes.	document notes that its purpose is to ensure that illion's complaints process complies with relevant industry codes.	

4.6 Subdivision G – Dealing with credit reporting information after the retention period ends

20V: Destruction of credit reporting information after the retention period ends

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
G.20V.0.1	N/A	Para 22, 22.1, 22.2 (a), (b)	illion must maintain adequate records to evidence their compliance with Part IIIA, the Regulations and the CR Code, in particular: • where credit-related personal information is destroyed to meet legislative obligations (but only if possible) • for credit reporting information disclosures by illion: the date of the disclosure, a brief description of the type of information disclosed, the credit provider, affected information recipient ('AIR') or other person to whom the disclosure was made and evidence that the disclosure was permitted under Part IIIA, the Regulations or the Code • records of any consent provided by an individual for the purposes of Part IIIA, the Regulations or the CR Code.	During stakeholder discussions, we were informed that credit reporting information is only retained for the time period as per the Act and the CR Code requirement or till the purpose is being fulfilled. Further, we were informed that CCB database records that are due for deletion are staged for 30 days and then deleted. Physical records are destroyed, and destruction confirmation certificates are provided. Inspected the document containing information of the records removed from CCB for Jan, Feb and March 2021, and noted that it contains the number of records which were archived and the number of records which were deleted from the CCB database, by 'information type' (e.g. bankruptcies deleted, accounts deleted, accesses deleted, etc) and by date.	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			• Records must be retained for a minimum period of 5 years from the date on which the record is made unless, the record includes information that illion is required by Part IIIA, the Regulations or the CR code to destroy at the end of the applicable retention period, in which case the record must be retained for the duration of that retention period only.	Inspected destruction certificates and noted that destruction of physical documents is recorded. Inspected the walkthrough document for deletion of files located on file servers and noted that following a request raised to delete records on file servers greater than illion's retention period, files that do not fall in the excluded documents will be identified and destruction is then recorded. Inspected sample of BAU diary showing data deletion schedules for electronic files, held discussions with stakeholders, and noted that data deletion occurs quarterly with the next event scheduled for 2 August 2021. Further, it was noted during stakeholder discussions, that there is no documents/ records disposal or destruction register to capture the following details: 1) records destruction request number; 2) record type (CCB data, hard copy data, working files, etc.); 3) authorised person; 4) date of request being raised; 5) date of request being completed; 6) reason for destruction; 7) approval for destruction; 8) method of destruction; and 9) evidence of destruction (as applicable).	

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
				The above point was discussed with illion management. illion management advised that they believe there is a minimal business risk and don't have any plans to change the current process as maintaining a log of hard copy documents that have been destroyed is not practical.	
G.20V.0.2	Div 2, Sec 20B (3) & (4), 20V, 20W, 20X, 20Y, 20Z and 20ZA	Para 1.2(f)	illion must destroy credit information and any related CRB-derived information or ensure that this information is de-identified within 1 month after the relevant retention period, unless: • immediately before the retention period ends there is a pending correction request in relation to the information; or • immediately before the retention period ends there is a pending dispute in relation to the information; or • if illion is required by Australian law or a court / tribunal order to retain the information. The prescribed retention periods range from 2 to 7 years, depending on the nature of the information, as per sections 20W, 20X, 20Y and 20Z of the Act. There is no retention period for identification information or credit information that is publicly available information about the individual that relates to the individual's activities in Australia or the external Territories, and the individual's credit worthiness and that is not court proceedings information about the individual or information about the	During stakeholder discussions, it was noted that CCB database records that are due for deletion are staged for 30 days and then deleted. Physical records are destroyed, and destruction confirmation certificates are provided. Inspected the Consumer Risk Solution (**CRS**) Data Retention, Archiving and Data Destruction Policy and noted that this Policy includes retention periods and codes for archiving and a destruction process, which relates to CRS data only. Further, it was noted that this document was dated May 2018 and has not been reviewed since. Inspected the IT Policy for Data Retention Compliance and noted that there is a requirement in the policy for a sweep to be performed of any files across all file servers that have not been modified for a period longer than 7 years, following which those files should be destroyed or de-identified, in order to keep in line with the retention period. It was noted that there is a practice of disposing of physical documents when no longer required or when their retention period has expired. However, a physical document disposal process has not been formalised.	 Minor improvement opportunity noted. *Refer to Section 3.2.*

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
			individual that is entered or recorded on the National Personal Insolvency Index. An obligation on illion to "destroy" credit information or credit reporting information requires illion to ensure it irretrievably destroys the information. Where it is not possible to irretrievably destroy credit-related personal information held in electronic format, illion should take steps to put the information 'beyond use.' In cases where illion holds credit reporting information that relates to consumer credit and it is satisfied that the individual has been a victim of fraud (including identity fraud) and consumer credit was provided as a result of that fraud, illion must destroy the credit reporting information, and within a reasonable period after the information is destroyed: • give the individual a written notice that states that the information has been destroyed and sets out the effect of the notification of destruction to prior recipients of the information • give the CP a written notice that states that the information has been destroyed. illion is not obliged to destroy the credit reporting information or notify prior recipients of the information of the destruction if illion is required by or under an Australian law, or a court / tribunal order, to retain the credit reporting information or not give such notification.	Inspected two sample emails of two different instances where a CP had been provided with a written notice from illion to state that fraudulent information had been destroyed from illion's system. Inspected two sample emails of two different instances where an individual had been provided with a written notice from illion to state that fraudulent information had been destroyed from illion's system.	

4.7 Additional requirement: Independent review of compliance

Ref #	Part IIIA Ref	CR Code Ref	Summary of Obligations and Existing Controls	Testing and Outcomes	Compliance Status
IRC.0.1	N/A	Para 24.2	Every 3 years or more frequently if the Commissioner requests, illion must commission an independent review of its operations and processes to assess compliance by illion with its obligations under Part IIIA, the Regulations and the CR code.	It is noted that illion had commissioned an independent review of its operations and processes to assess compliance by illion with its obligations under Part IIIA, the Regulations, and the CR code in 2017. The next review was scheduled for 2020. However, due to the COVID-19 pandemic, the review was postponed until 2021. illion has commissioned an independent review of its operations and processes to assess compliance by illion with its obligations under Part IIIA, the Regulations, and the CR code.	
IRC.0.2	N/A	Para 24.2	illion must consult with the Commissioner as to the choice of reviewer and scope of the review.	It is noted that illion had consulted with the Commissioner about the choice of the reviewer and the scope of the review for the year 2021.	
IRC.0.3	N/A	Para 24.2	The review report and illion's response to the review report must be provided to the Commissioner and made publicly available.	It was noted that in the year 2017, illion had provided the review report and response to the review report to the Commissioner and made it publicly available.	

Appendices

Appendix A - Documents received

The following table represents documents received in producing this report.

To maintain an agreed source of truth of the information provided by illion and considered by KPMG in the completion of our work related to the preparation of this report, only documents formally provided have been included below.

Document title
[Document titles withheld]

Document title
[Document titles withheld]

Document title
[Document titles withheld]

Document title
[Document titles withheld]

Document title
[Document titles withheld]

Document title
[Document titles withheld]

Document title
[Document titles withheld]

Document title
[Document titles withheld]

Appendix B - List of illion personnel

Discussions and workshop were held with the following illion personnel.

Name	Designation
[Personal information withheld]	Privacy Compliance Officer
	Financial Controller
	Head of Client Operations
	Senior Manager, Consumer Data
	IT Risk and Security Analyst
	PAC Team Leader
	PAC Team Leader