



Independent review of compliance with
Part IIIA of the Privacy Act 1988 and the
Privacy (Credit Reporting) Code 2014
(Version 2.3)

illion Australia Pty Ltd

12 December 2024
kpmg.com.au

Inherent Limitations

As set out in our Engagement Letter dated 22 April 2024 (**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 2.3) (**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 15 August 2024 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

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 22 April 2024. 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 consent to this report being released to the OAIC and illion's website on the basis set out in our Engagement Letter.

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 inaccuracies appearing in any reproduction in any form or medium.



Contents

- 1 Executive summary 4
- 1.1 Introduction 4
- 1.2 Background 4
- 1.3 Scope 4
- 1.4 Limitations 4
- 2 Overall Conclusion 5
- 2.1 Compliance Status 5
- 3 Findings 7
- 3.1 Subdivision B – Consideration of information privacy 7
- 3.2 Subdivision C – Collection of credit information 10
- 3.3 Subdivision D – Dealing with credit reporting information 13
- 3.4 Subdivision E – Integrity of credit reporting information 18
- 3.5 Subdivision F – Access to and correction of information 26
- 3.6 Additional requirement: Independent review of compliance 35
- Appendix 1: List of policies/procedures/documents received 36
- Appendix 2: List of illion personnel 44
- Appendix 3: Methodology 45

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 2.3) (**CR Code**). This report considers those obligations only and not the Australian Privacy Principles.

As set out in our Engagement Letter dated 22 April 2024, KPMG has undertaken an independent review of illion's compliance with the Privacy Act, the Regulations and the CR Code and produced a report including a summary of compliance status.

This report supersedes the previous report dated 30 August 2024 which was made available on illion's website.

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:

- 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 and the CR Code, and other guidelines, which may differ from the subsequent interpretation of those laws, regulations and guidelines by OAIC.
- KPMG does not warrant the accuracy or reliability of any of the information supplied to it in the course of this engagement.
- 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.
- Review of the Information Security Management System (**ISMS**) and Business Continuity Management System (**BCMS**) framework is not part of the scope.
- Responsibility for the security of any electronic distribution of this report remains the responsibility of illion.
- KPMG accepts no liability if the report is or has been altered in any way by any person.
- KPMG's role does not include any explicit or implicit approval functions or responsibilities.

2 Overall Conclusion

Overall, the design of illion’s operations and control processes complies 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 among illion’s employees regarding the business’s obligations under the Privacy Act, the Regulations, and the CR Code, which is consistent with the overarching policies and procedures at illion and reiterates 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 testing approach also included review of assurance reports as it relates to illion’s handling of credit information as applicable and outlined in the Summary of Obligations under Findings in Section 3. Our review identified one minor improvement opportunity in relation to documenting approval or periodic reviews for some of the illion policy/procedure documents that support handling of credit information. These have been discussed with illion management, who are committed to addressing it.




2.1 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 <i>B.20B.0.2</i> (Refer to Section 3.1)
4.2	Sections 20C, D & L	Para 5, 6, 7, 8, 9, 10, 11 and 12	Subdivision C – Collection of credit information	
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	
4.4	Sections 20 N & Q	Para 2, 5, 15 and 23	Subdivision E – Integrity of credit reporting information	

Report Ref.	Part IIIA Ref.	CR Code Ref.	Subdivision	Compliance Status
4.5	Sections 20 R, S, T, U & Div 5 S23	Para 19, 20 & 21	Subdivision F – Access to and correction of information	
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	
4.7	N/A	Para 24	Additional requirement: Independent review of compliance	




3 Findings

The following table sets out:




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

3.1 Subdivision B – Consideration of information privacy

20B: Open and transparent management of credit reporting information

Ref #	B.20B.0.1	B.20B.0.2	B.20B.0.3
Part IIIA Ref	Div 2, Sec 20B (3) & (4)	Div 2, Sec 20B (2)	Div 2, Sec 20B (5)
CR Code Ref	Para 3	Para 3	Para 3 & 3.1
Compliance Status		 Minor improvement opportunity noted	
Summary of Obligations	<p>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:</p> <ul style="list-style-type: none"> • 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 direct marketing, and how an individual can request to not use their information for pre-screening purposes; 	<p>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.</p> <p>illion has credit reporting related policies, processes and procedures documented and has them periodically reviewed.</p>	<p>illion must make its Credit Reporting Policy available for free and publish the policy on its website.</p>



Ref #	B.20B.0.1	B.20B.0.2	B.20B.0.3
	<ul style="list-style-type: none"> 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. 		



Ref #	B.20B.0.4	B.20B.0.5	B.20B.0.6
Part IIIA Ref	Div 2, Sec 20B (2)	N/A	Div 2, Sec 20B (2)
CR Code Ref	Para 3	Para 2.2 (a),(b)	Para 3
Compliance Status			
Summary of Obligations	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> 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; 	<p>illion must take reasonable steps to:</p> <ul style="list-style-type: none"> 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. 	<p>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.</p> <p>Credit reporting risks are included in illion's risk statement.</p>

Ref #	B.20B.0.4	B.20B.0.5	B.20B.0.6
	<ul style="list-style-type: none"> • 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); liaising with relevant credit reporting bodies; and cooperating with appropriate regulators.. 		


3.2 Subdivision C – Collection of credit information

20C: Dealing with solicited credit information

Ref #	C.20C.0.1	C.20C.0.2
Part IIIA Ref	Div 2, Sect 20C	Div 2, Sec 20C(4)(e)
CR Code Ref	Para 5.1(a), 5.2, 5.4(a), (b) & (c), 6, 7, 8, 9, 10 and 12	Para 8
Compliance Status		
Summary of Obligations	<p>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).</p> <p>Where the information collected from a CP is:</p> <ul style="list-style-type: none"> • 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. <p>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:</p> <ul style="list-style-type: none"> • use the information disclosed by CPs in relation to individuals' dates of birth to identify any information disclosed by a CP that: <ul style="list-style-type: none"> – 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. 	<p>illion is permitted to collect RHI from the CP, if the CP is a licensee or is prescribed by the Regulations.</p> <p>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.</p>




Ref #	C.20C.0.1	C.20C.0.2
	<ul style="list-style-type: none"> as soon as practicable identify whether collected information includes information that illion is 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. 	
Ref #	C.20C.0.3	C.20C.0.4
Part IIIA Ref	Div 2, Sec 20L	N/A
CR Code Ref	N/A	Para 11 & 11.1
Compliance Status		
Summary of Obligations	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.	illion must only collect publicly available information about an individual: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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).

20D: Dealing with unsolicited credit information

Ref #	D.20D.0.1
Part IIIA Ref	Div 2, Sec 20D
CR Code Ref	N/A
Compliance Status	
Summary of Obligations	<p>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.</p> <p>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.</p>

3.3 Subdivision D – Dealing with credit reporting information

20E: Use and disclosure of credit information



Ref #	D.20E.0.1	D.20E.0.2	D.20E.0.3
Part IIIA Ref	Div 2, Sec 20E (1) & (2)	Div 2, Sec 20E (5)	Div 2, Sec 20E, 20F and 20P
CR Code Ref	N/A	Para 22 (c)	Para 7, 8, 9, 12,14 and 16
Compliance Status			
Summary of Obligations	<p>illion is permitted to use credit reporting information in the following ways:</p> <ul style="list-style-type: none"> 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. 	<p>illion must have a process to ensure that a written note is made of all disclosures of credit-related information. Including:</p> <ul style="list-style-type: none"> The date of the disclosure; A brief description of the type of information disclosed; The credit provider, affected information recipient, or other person to whom the disclosure was made; and <ul style="list-style-type: none"> Evidence that the disclosure was permitted under Part IIIA of the Act. 	<p>illion is permitted to disclose credit reporting information about an individual if:</p> <ul style="list-style-type: none"> 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. <p>The CR Code also provides the conditions under which illion can disclose certain credit information, i.e:</p> <ul style="list-style-type: none"> Para 7 – Where a CP makes an information request to illion in connection with an application for consumer credit and the amount

Ref #	D.20E.0.1	D.20E.0.2	D.20E.0.3
			<p>of credit is unknown or incapable of being specified, the credit information that illion may collect and disclose may include that an unspecified amount of consumer credit is being sought from the CP.</p> <ul style="list-style-type: none"> • 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 than \$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: <ul style="list-style-type: none"> – the CP confirms to illion that it is aware of circumstances that reasonably



Ref #	D.20E.0.1	D.20E.0.2	D.20E.0.3
			<p>indicate that the individual may be at significant risk of defaulting in relation to those obligations; or</p> <p>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.</p>

Ref #	D.20E.0.4	D.20E.0.5	D.20E.0.6
Part IIIA Ref	Div 2, Sec 20P	Div 2, Sec 20M (1) & (2)	Div 2, Sec 20G (5), (6) and (7)
CR Code Ref	N/A	N/A	N/A
Compliance Status			
Summary of Obligations	<p>illion must not use or disclose credit reporting information that is materially false or misleading, unless:</p> <ul style="list-style-type: none"> 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. 	<p>illion may use or disclose de-identified credit reporting information in the following circumstances:</p> <ul style="list-style-type: none"> the use or disclosure is for the purposes of conducting research in relation to credit; and <ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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

Ref #	D.20E.0.4	D.20E.0.5	D.20E.0.6
			have made a request not to receive direct marketing.

Ref #	D.20E.0.7	D.20E.0.8
Part IIIA Ref	Div 2, Sec 20H, 20J	Div 2, Sec 20K
CR Code Ref	N/A	N/A
Compliance Status		
Summary of Obligations	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • 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.

20K: Protections for victims of fraud

Ref #	D.20K.0.1	D.20K.0.2
Part IIIA Ref	Div 2, Sec 20K (1), (2) & (3)	N/A
CR Code Ref	Para 17.1 and 17.3	Para 17.2
Compliance Status		
Summary of Obligations	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	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.

Ref #	D.20K.0.1	D.20K.0.2
	<p>requests illion not to use or disclose credit reporting information about them, unless:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> – 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 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. 	




Ref #	D.20K.0.3	D.20K.0.4
Part IIIA Ref	Div 2, Sec 20K (4) & (5)	Div 2, Sec 20K (6)
CR Code Ref	N/A	N/A
Compliance Status		
Summary of Obligations	<p>If the individual requests an extension to the ban period (of 21 days) before the period ends, and illion believes on reasonable grounds that the individual has been, or is likely to be, a victim of fraud (including identity fraud) illion must:</p> <ul style="list-style-type: none"> 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. 	<p>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.</p>

3.4 Subdivision E – Integrity of credit reporting information

20N: Quality of credit reporting information




Ref #	E.20N.0.1
Part IIIA Ref	Div 2, Sec 20N
CR Code Ref	Para 5.4(d), (e) & (f)
Compliance Status	
Summary of Obligations	<p>illion must take reasonable steps in the circumstances to ensure that the credit information it collects, uses and discloses is aligned to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.</p>

20Q: Security of credit reporting information

Ref #	E.20Q.0.1	E.20Q.0.2	E.20Q.0.3
Part IIIA Ref	Div 2, Sec 20Q (1)	Div 2, Sec 20Q (1) & (3)	Div 2, Sec 20Q (1)
CR Code Ref	Para 15.1	N/A	N/A
Compliance Status			
Summary of Obligations	<p>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.</p> <p>illion must maintain reasonable practices, procedures and systems to ensure the security of electronic transmission and storage of credit reporting information.</p> <p>illion has the following controls in place:</p> <ul style="list-style-type: none"> 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 	<p>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.</p> <p>illion must maintain reasonable practices, procedures and systems to ensure the security of electronic transmission and storage of credit reporting information.</p> <p>illion must store the credit reporting information it holds:</p> <ol style="list-style-type: none"> either: <ol style="list-style-type: none"> in Australia or an external Territory; or in accordance with any security requirements prescribed by the regulations for storing the information outside of Australia and the external Territories; and in accordance with any security requirements prescribed by the regulations. <p>illion has the following technical security controls in place:</p>	<p>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.</p> <p>illion must maintain reasonable practices, procedures and systems to ensure the security of electronic transmission and storage of credit reporting information.</p> <p>illion has the following controls in place around mobile devices (including BYOD) of employees and contractors, such as:</p> <ul style="list-style-type: none"> 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 <p>illion's ASAE (SOC 2) report for the period of 1 Jan 2023 to 31 Dec 2023, noted exceptions related to user access management. Whilst these user accounts retained access, these users were not</p>

Ref #	E.20Q.0.1	E.20Q.0.2	E.20Q.0.3
	<p>risks, including threats and vulnerabilities the potential impacts of these risks to information (including personal information) handled by an entity.</p> <ul style="list-style-type: none"> • 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. • 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. 	<ul style="list-style-type: none"> • 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 • 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 	<p>able to access the application after their termination date as their network access was removed or did not access Windows AD after their termination date. A detailed review of user access provisioning and de-provisioning for the period of 1 Jan 2024 to 30 Jun 2024) of users with access to CCB systems noted that access was granted after proper approvals and terminated on the last day of employment.</p>


Ref #	E.20Q.0.1	E.20Q.0.2	E.20Q.0.3
	<ul style="list-style-type: none"> • 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. • 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. 	<p>of bulk data, for example through the use of personal storage devices.</p> <ul style="list-style-type: none"> • illion has restricted access areas controlled and managed (specifically for the facilities housing systems storing/processing Personal Information and communications equipment controlling its transfer). 	

Ref #	E.20Q.0.4	E.20Q.0.5	E.20Q.0.6
Part IIIA Ref	Div 2, Sec 20Q (1)	Div 2, Sec 20Q (1)	Div 2, Sec 20N (3) and 20Q (2)
CR Code Ref	N/A	N/A	Para 2.1 and 15
Compliance Status			
Summary of Obligations	<p>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.</p> <p>Illion must maintain reasonable practices, procedures and systems to ensure the security of electronic transmission and storage of credit reporting information.</p> <p>Illion has the following controls in place around third parties:</p> <ul style="list-style-type: none"> • 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. 	<p>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.</p> <p>Illion must maintain reasonable practices, procedures and systems to ensure the security of electronic transmission and storage of credit reporting information.</p> <p>Illion has the following controls in place around physical document security:</p> <ul style="list-style-type: none"> • a 'clean desk' policy. • procedures governing the printing of documents containing personal information. • physical security controls (e.g. access cards) in place to prevent unauthorised access to premises and systems. 	<p>Illion must enter into written agreements with CPs that require the providers to:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • misuse, interference and loss; and • unauthorised access, modification, or disclosure. <p>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.</p>

Ref #	E.20Q.0.4	E.20Q.0.5	E.20Q.0.6
	<ul style="list-style-type: none"> Illion reports the results of third party monitoring and assurance regularly to management. 		



Ref #	E.20Q.0.7	E.20Q.0.8	E.20Q.0.9
Part IIIA Ref	N/A	Div 2, Sec 20N (3)(b) & (c) and 20Q (2)(b) & (c)	N/A
CR Code Ref	Para 23.1 & 23.2	Para 23.1, 23.3, 23.4, 23.5 & 23.6	Para 5.4(g)
Compliance Status			
Summary of Obligations	<p>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:</p> <ul style="list-style-type: none"> 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 	<p>Illion must:</p> <ul style="list-style-type: none"> 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. <p>Illion's risk based program must include a CP audit program for CPs to assess compliance with their obligations to ensure that:</p> <ul style="list-style-type: none"> 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 	<p>Where Illion identifies credit information that is not accurate, up-to-date and complete, raise this, where reasonable, with the CP that disclosed the information and request the CP to:</p> <ul style="list-style-type: none"> 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



Ref #	E.20Q.0.7	E.20Q.0.8	E.20Q.0.9
	<ul style="list-style-type: none"> • 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. 	<p>required by Part IIIA of the Act, the CR Code and the Regulations.</p> <ul style="list-style-type: none"> • 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 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. <p>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.</p> <p>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.</p>	<p>CP) by illion as referred to in section 20N(3) and section 20Q(2) respectively.</p>

Ref #	E.20Q.0.10
Part IIIA Ref	N/A
CR Code Ref	Para 23.11
Compliance Status	
Summary of Obligations	<p>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:</p> <ul style="list-style-type: none"> • Access & Corrections • Complaints • Serious credit infringements • illion's monitoring and auditing activity • Disclosure of CCLI and RHI to illion <p>Any other information requested by the Commissioner</p>




3.5 Subdivision F – Access to and correction of information




20R: Access to credit reporting information

Ref #	F.20R.0.1	F.20R.0.2
Part IIIA Ref	Div 2, Sec 20R (1), (2) & (3)	Div 2, Sec 20R (4)
CR Code Ref	Para 19.1 & 19.2	Para 19.4 & 19.6
Compliance Status		
Summary of Obligations	<p>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.</p>	<p>For access free of charge, illion must provide the access seeker with access to:</p> <ul style="list-style-type: none"> 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. <p>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.</p> <p>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.</p>




Ref #	F.20R.0.3	F.20R.0.4
Part IIIA Ref	Div 2, Sec 20R (2) & (7)	Div 2, Sec 20R (6)
CR Code Ref	N/A	Para 19.3
Compliance Status		
Summary of Obligations	<p>illion is not required to give an access seeker access to credit reporting information if:</p> <ul style="list-style-type: none"> 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. <p>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:</p> <ul style="list-style-type: none"> 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. 	<p>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.</p> <p>Where illion has a fee-based service for providing an access seeker with credit reporting information:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 <p>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.</p>


20S: Correction of credit reporting information

Ref #	F.20S.0.1	F.20S.0.2	F.20S.0.3
Part IIIA Ref	Div 2, Sec 20S (1), 20T (2), (3) & (4) and 20U	N/A	N/A
CR Code Ref	Para 20.4	Para 20.2 (a)	Para 20.3
Compliance Status			
Summary of Obligations	<p>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:</p> <ul style="list-style-type: none"> 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. <p>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.</p>	<p>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.</p>	<p>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:</p> <ul style="list-style-type: none"> 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. <p>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.</p>




Ref #	F.20S.0.4	F.20S.0.5	F.20S.0.6
Part IIIA Ref	N/A	Div 2, Sections 20S (2) & (3) and 20U (2), (4) & (5)	Div 2, Sections 20 S (2), 20U (2)
CR Code Ref	Para 20.5 & 20.6	Para 20.7	Para 20.7 & 20.9
Compliance Status			
Summary of Obligations	<p>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.</p>	<p>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:</p> <ul style="list-style-type: none"> The individual the correction relates to the interested party, i.e. the CP or CRB it consulted with (if applicable) regarding a correction request <p>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.</p>	<p>The notice to the individual must:</p> <ul style="list-style-type: none"> 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 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. <p>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:</p> <ul style="list-style-type: none"> All CRBs to which it disclosed the pre-corrected information;

Ref #	F.20S.0.4	F.20S.0.5	F.20S.0.6
			<ul style="list-style-type: none"> 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.




Ref #	F.20S.0.7	F.20S.0.8	F.20S.0.9
Part IIIA Ref	N/A	N/A	Div 2, Sec 20T (5)
CR Code Ref	Para 20.9	Para 20.8	N/A
Compliance Status			
Summary of Obligations	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 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.	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.	illion must not charge the individual for requesting the correction or for correcting the information.

Ref #	F.20S.0.10
Part IIIA Ref	Div 2, Sec 20U (3)
CR Code Ref	N/A
Compliance Status	
Summary of Obligations	<p>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:</p> <ul style="list-style-type: none"> 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 <p>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.</p>

23B: Dealing with complaints



Ref #	F.23B.0.1	F.23B.0.2	F.23B.0.3
Part IIIA Ref	Div 5, Sec 23B (1) and 23C (2)	N/A	Div 5, Sec 23C (4)
CR Code Ref	Para 21.3 & 21.5	Para 21.4	N/A
Compliance Status			
Summary of Obligations	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	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:	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

Ref #	F.23B.0.1	F.23B.0.2	F.23B.0.3
	<p>the complaint and make a decision about the complaint. Specifically, illion must:</p> <ul style="list-style-type: none"> 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 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. <p>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.</p> <p>Unless it is impracticable or illegal to give notice to a CP about a complaint relating to a CRB's act of</p>	<ul style="list-style-type: none"> 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. 	<p>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.</p>

Ref #	F.23B.0.1	F.23B.0.2	F.23B.0.3
	practice that may breach Section 20S, this obligation is taken to be met if illion gives notice as soon as practicable to: <ul style="list-style-type: none"> 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 any other CP that has been nominated by the individual for this purpose. 		
Ref #	F.23B.0.4	F.23B.0.5	F.23B.0.6
Part IIIA Ref	Div 5, Sec 23A (5)	N/A	Div 2 Sec20B 2(b)
CR Code Ref	N/A	Para 21.2	N/A
Compliance Status			
Summary of Obligations	illion must not charge the individual for making of the complaint or for dealing with the complaint.	illion must be a member of a recognised EDR scheme.	illion must have documented policies, processes and procedures in place for receiving and dealing with privacy inquiries or complaints from individuals. illion has a complaints process complying with relevant industry codes.




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

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

Ref #	G.20V.0.1	G.20V.0.2
Part IIIA Ref	N/A	Div 2, Sec 20B (3) & (4), 20V, 20W, 20X, 20Y, 20Z and 20ZA
CR Code Ref	Para 22, 22.1, 22.2 (a), (b)	Para 1.2(f)
Compliance Status		
Summary of Obligations	<p>illion must maintain adequate records to evidence their compliance with Part IIIA, the Regulations and the CR Code, in particular:</p> <ul style="list-style-type: none"> 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. <p>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.</p>	<p>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:</p> <ul style="list-style-type: none"> 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. <p>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 individual that is entered or recorded on the National Personal Insolvency Index.</p> <p>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.'</p> <p>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:</p>

Ref #	G.20V.0.1	G.20V.0.2
		<ul style="list-style-type: none"> • 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.

3.6 Additional requirement: Independent review of compliance

Ref #	IRC.0.1	IRC.0.2	IRC.0.3
Part IIIA Ref	N/A	N/A	N/A
CR Code Ref	Para 24.2	Para 24.2	Para 24.2
Compliance Status			
Summary of Obligations	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.	illion must consult with the Commissioner as to the choice of reviewer and scope of the review.	The review report and illion's response to the review report must be provided to the Commissioner and made publicly available.

Appendix 1: List of policies/procedures/documents received

The following table represents documents received when producing the Report.

To maintain an agreed source of truth regarding the information provided by Lillion and considered by KPMG in completing our work related to preparing the Report, only documents formally provided have been included below.

Document reference (if applicable) and document title
1 illion Credit Reporting Policy October 2023 clean
2 AFCA Procedure & Work Instruction 1.0 2 CMS Procedure & Work Instruction 1.1 2 Complaints Handling Procedure - illion 2 PAC Operator Telephone Complaints Procedure & Work Instruction 1.1
4. Privacy-Impact-Assessment-Template-Sept-2020
5. Data-PI-Retention-Policy-Feb-2024-final
6. & 7. & 50. Data-Breach-Cyber-Incident-Response-Plan-March-2024
<ul style="list-style-type: none"> • Australian Privacy 2024 - https://trainingpreview.edapp.com/p/zBUtQdQb1QEtzpVoujGsZWSs • Cyber Security @ illion – Security outside the office 2024 - https://trainingpreview.edapp.com/p/6JZuUaM07h2lrG2Ee82VUKuz • Cyber Security awareness @ illion – 2024 - https://trainingpreview.edapp.com/p/MCmcTFTCaKiQHQ2jFYuQTPEW • Information Security and Acceptable use policy – 2024 - https://trainingpreview.edapp.com/p/dYJ9QH050D0jUpAR4rZ6Uk6a • Information Classification and Handling – 2024 - https://trainingpreview.edapp.com/p/dojIB6FafMmmHBwxugcPxqq8
9. illion-Policy-Information-Security-v3.9-1

Document reference (if applicable) and document title
10. Risk-Management-Policy-2023
11 CCB DQ Procedures v4.3
12 Consumer Bureau - Australia
13 AU Bureau Contributors - Mar_24
14. CR Portal Setup Guide 14. Procedure - Direct data load via SFTP 14. CR Portal Setup Guide 14. Procedure - Direct data load vis SFTP 14Client-Direct to Bureau CCR Data Load - Internal Project Process Map-100624-230852 (1) 14Client-Direct to Bureau CCR Data Load - Internal Project Process Map-100624-230852
15 illion Consumer Schema CCR (FULL) User Guide
16 CCB Batch Technical Documentation - Product BBC6 - V4.0_illion 16 CCB Batch Technical Documentation - Product BBC8 - V0.5_illion
17 TPO - Dataflow Compliance - Steerco - June_23_2022_WIP
18 CCB DQ Procedures v4.3
19 CCB-Technical_Information_Pack-V3.16_AU202012-AllProductsVersion_illion 19 Subscribers Statistics Report - June 2024
Sample Consumer Credit Report Screenshot
21 AFCA Complaint records received_closed
22 AU and NZ CCR RHI 2024-05-02
[Entity name redacted] [Entity name redacted] MSA

Document reference (if applicable) and document title
23 [Entity name redacted] _Standard Terms v10_3 (09-14)
23 [Entity name redacted] -Consumer Credit Services (AUST)-Services Agreement dated 1 October 2015
23 [Entity name redacted] -WOB Variation Letter Agreement No. 1 dated 1 October 2016
23 [Entity name redacted] -WOB Variation No. 2 and 3-dated 25 October 2019
23 [Entity name redacted] - WORK ORDER RMS CONSUMER RISK SERVICES 22.4.2021
23 [Entity name redacted] -MSA 00089777-18 Feb 2020
23 [Entity name redacted] -PRODUCT SCHEDULE R&MS - AU CONSUMER RISK SERVICES
24 Alerts & Monitoring User Guide v0.4
24 AM Alerts & Monitoring Specs v1.1
27 ClearScore Correction AU Procedure & Work Instruction 1.0
27 DBTB Default Removal & Update AU Procedure & Work Instruction 1.0
27 Default Conversion Process
27 Illion Corrections AU Procedure & Work Instruction 1.0
27 Mail Merge Procedure & Work Instruction 1.0
27 Manual Applications Procedure & Work Instruction 1.1
27 Manual ID Verification AU & NZ Procedure & Work Instruction 1.1
27 Manual Triage Procedure & Work Instruction 1.2
27 Regular Mail Procedure & Work Instruction 1.0
27 Untangling AU & NZ Procedure & Work Instruction 1.0
28 Manual Bans and Manual Suppressions Procedure & Work Instruction 1.1
29 Current File Bans as at 2024_06_12
30 CCB Bans TXn Examples AU
31 AU_CCR_DataQuality_CBA_BB
31 Consumer bureau pack April 2024
32 2023 FINAL CDS SOC 2 Report 210324

Document reference (if applicable) and document title
33 Appendix 2 - Risk Management Policy 2023
34 Evidence of Enterprise Risk Register Update to the illion Board
35. illion-BCMS-Crisis-Management-Plan-v3.1-1 35. illion-BCMS-Policy-and-Framework-v2.2
36 illion BCP Test - CRS - Approved 36 illion Business Unit BCP (CRS) v3.6 - Customer Version 36 illion DR Test - CCB - Customer Version
37 Companywide-Compliance-Training-2023 (1) 37 course-completion-by-user - Annual Compliance
38 Screen Shot - [Staff name redacted]
39. illion-Policy-Access-Management-v4.4 39 CCB-Data-Access-Policy-Oct-2023 (1)
40 Privileged Access Review - Evidence 40 [Staff name redacted] CCB Access Ticket 40 New Hires from 1st March 2024 to 11 June 2024
41 Terminations - April 2024 41 Terminations - March 2024 41 Terminations - May 2024 41 [Entity name redacted] 41 [Entity name redacted] 41 [Entity name redacted] MSA 41 [Entity name redacted] Limited
42 Non Priv Access Review - Inactive Directory Accounts - Evidence 42 Non Priv Access Review - Monthly Staff OnOff Boarding Review - Evidence 42 Non Priv Access Review - Quarterly Role Reconciliation - Evidence 42 Non Privileged Access Review - Full Report 2024
43. illion-Policy-IT-Change-Management-v2.3

Document reference (if applicable) and document title
44 List of changes made to Consumer Credit Bureau systems 44 List of changes made to Consumer Credit Bureau systems 44 Change Management Change Request evidence
45. illion-Policy-Backup-and-Recovery-v3.6 (1)
46 Backup History - Evidence
47. illion-Policy-Vulnerability-Management-v6.0 47 Vulnerability Management Report - Evidence
48 CIO Weekly Report - Evidence 48 ILLION - CCB - Web Pen test
Illion Website
50. Data-Breach-Cyber-Incident-Response-Plan-March-2024 (1)
51 Privacy Incident Register truncated 2024 51 Privacy Incident Supporting documents 2024 51 Privacy Incident Supporting documents location
52 Encryption Backup, SAN, workstation 12102024
53 CCB high-level network security diagram
54 security architecture diagram
55 Workstation Policy
56 illion Default Domain Policy
57 illion Credit Check ID Registration Documents 57 illion Credit Check set up
58. illion-Policy-Remote-Access-v4.9

Document reference (if applicable) and document title
59 USB Group Policy
60. & 65. illion-Policy-Physical-Security-v4.8
61. illion-Policy-Mobile-Devices-v5.4
62. illion-Policy-Third-Party-Management-v4.8
63 FY 24 Supplier Assessment Calendar - Evidence 63 GRC SC 23 Apr 2024 Truncated
64 illion Procurement Policy - May 2024 - signed 64 illion-Procurement-Procedure-Purchase-to-Pay-Products-and-Fixe 64 illion-Procurement-Procedure-Purchase-to-Pay-Variable-Costs-June-2021
60. & 65. illion-Policy-Physical-Security-v4.8
66 CRB Risk Based Monitoring Program Oct 2019
67 Manual ID Verification AU & NZ Procedure & Work Instruction 1.1
20 & 69 CYCAU_UserAudit_20240616_Signups redacted
70 How to determine what caused a mix-up 70 Illion Corrections AU Procedure & Work Instruction 1.1 70 Manual Corrections where the CP requires encrypted mail Procedure & Work Instruction 1.0
71 AU CCR Accounts deleted 71 AU default removals 71 AU Enquiry deletions 71 AU judgements and summons deletion and updates
72 202404 Privacy Framework - Steering Committee Apr 2024 Redacted
73. illion-Secure-Destruction-Procedure-September-2021-1 73 CRS Data Retention Archiving and Data Destruction Policy V1.0 May 2018 - Copy

Document reference (if applicable) and document title
74 2024_06_06 Sample_Accounts Archiving after 2 years of closed Date
75 DisputeExtract_20240604 75 Correction notice - [Name redacted] 10122397 75 Correction notice - [Name redacted] 10122397 75 Correction Notice - [Name redacted] 8477486 (1) 75 Correction Notice - [Name redacted] 8477486 75 Corrections Notice example 2 75 Corrections Notice
76. illion-Complaint-Handling-Policy-October-2023-clean 76 CMS Procedure & Work Instruction 1.1 76 PAC Operator Telephone Complaints Procedure & Work Instruction V1.1 76 illion Complain Handling Policy May 2024 clean
77 investigated-users_view 77 investigating-users-view
78. MemberCertificate
79 CRS Data Retention Archiving and Data Destruction Policy V1.0 May 2018
80. Certificate Of Data Erasure ILI0023 80 20240604_Triennial audit Deleted ArchivedCounts
81 Example 1 part 1 20240611 81 Example 1 part 2 20240612 81 Example 2 part 1 20240611 81 Example 2 part 2 20240612
82 Credit Bureau - Credit Bureau Correction Request - 878864 (1) 82 Credit Bureau - Credit Bureau Correction Request - 878864 82 Credit Bureau - Credit Bureau Correction Request - 878917 (1) 82 Credit Bureau - Credit Bureau Correction Request - 878917
83. 20240118 Letter to Illion - Scope of independent review and choice of reviewer KPMG

Document reference (if applicable) and document title
84 illion-Policy-Acceptable-Use-v3.12
85 App Whitelisting - Evidence
86 illion Application List - Evidence
14. CR Portal Setup Guide 87 Client onboarding Process Map 87 Onboarding Procedure - Direct data load via SFTP v2.1
88 Onboarding {Company Name} MTF File Transfer
89 Onboarding FW ME CCR
90 Onboarding FW in1bank CCR data via CR portal - Data Quality Check
91 [Entity name redacted] CCR Data load illion Direct Handover 91 RE [Entity name redacted] - illion BAU Support Model
20240617 Employee Training
"100 illion Third Party Security Assessment Report - SKYC 100 illion Third Party Security Assessment Report [Verizon] MSSP"
103 DisputeExtract 7 May 2024
105 illion Corrections Handling Policy May 2024
107 illion Ban request extension template
Response received in the email dated 19th June 2024
Privacy Compliance officer role PD

Appendix 2: List of illion personnel

Discussions and workshops were held with the following illion personnel.

	Role
1	General Manager Consumer Risk
2	Integration Team Leader
3	Public Access Centre Lead
4	Public Access Centre Team Leader
5	Complaints Resolution Officer
6	Head of Information Security, Risk & Compliance
7	Senior Talent & Capability Partner
8	Manager Data Management
9	Technology Risk and Security Manager
10	Privacy Compliance Officer
11	General Manager Finance

Appendix 3: Methodology

In accordance with paragraph 24.2 of the CR Code, every three years (or more frequently, if the Commissioner requests), a Credit Reporting Body (**CRB**) must commission an independent review of its operations and processes to assess compliance by the CRB with its obligations under Part IIIA of the Privacy Act, the Regulations and the CR Code. In light of the requirement, KPMG conducted an independent review of illion's compliance with Part IIIA of the Privacy Act, the Regulations and the CR Code. A summary of the methodology broken down into steps was followed for the independent review:

Step 1: Initial Diagnostic

Key activities involved in this phase were:

- Identified key stakeholders for the Engagement.
- Held discussions with key stakeholders across the business who can access the credit information to identify touchpoints and understand existing processes and controls.
- Identified controls that overlap with Information Technology General Control (**ITGC**) testing and Service Organisational Controls (**SOC**) testing areas within this Engagement's scope.
- Identified additional controls that need to be assessed within the scope of this Engagement.
- Developed an initial document request list.
- Scheduled meetings with the identified key stakeholders to understand key controls for managing credit information.

Step 2: Review of Governance and Processes

Key activities involved in this phase were:

- Performed an independent review of the current business processes and credit reporting framework to determine any gaps that need to be addressed by undertaking the following:
 - Performed a walkthrough of credit reporting systems and authorised access levels.
 - Reviewed the credit information lifecycle to ensure it is accurate, up to date, and complete.
 - Reviewed processes and controls to disclose credit information.
 - Reviewed any risk profile/ risk assessment/ risk register(s) relating to credit reporting, privacy, and information security.
 - Reviewed Complaints and Incident handling policies.
 - Reviewed IT Security policies and controls.
 - Reviewed training material.

Step 3: Testing of Process Controls

Key activities involved in this phase were:

- Performed testing over the process and controls that illion has implemented to ensure compliance under Part IIIA of the Privacy Act and the CR Code.
- Testing involved performing an independent review (walkthrough) of the end-to-end credit reporting process (to be confirmed with you) to ensure all touchpoints where information is collected, held, used, and disclosed have been appropriately captured.
- To test the completeness of illion's compliance with illion's obligations, the processes selected for testing were a combination of high-priority processes and other processes identified in Step 2 by KPMG as potentially dealing with credit information.

Step 4: Reporting and Review of Action Plan

Key activities involved in this phase were:

- Prepared the draft report.
- Held discussions with the stakeholders on the draft report.
- Finalised the review report.