Equifax New Zealand Information Services and Solutions Limited

Assurance Report

Year ending 30 June 2022

Table of Contents

1. Introduction

Equifax New Zealand Information Services and Solutions Limited (**Equifax**) is a leading provider of credit information and data driven solutions in New Zealand.

Equifax's customers in New Zealand use data intelligence provided by Equifax to make decisions on credit risk, verify identity and employee background, reduce identity theft and fraud, and undertake marketing strategies.

Clause 8 of the Credit Reporting Privacy Code 2020 (**Code**) mandates that Equifax provide an annual report (this **Assurance Report**) to the Privacy Commissioner prepared in accordance with the requirements of Schedule 7 of the Code. Equifax is also required to provide supplementary information in relation to any "additional questions" requested by the Office of the Privacy Commissioner (**OPC**). Equifax has endeavoured to address all the requirements of the OPC Assurance Review through this Assurance Report.

This Assurance Report was prepared in line with Equifax's formal Compliance Program, a key component of which is an Assurance Review Committee constituted in accordance with clause 8(2)(b) of the Code (**Assurance Review Committee**), which includes an independent person with expertise in relation to matters of Code compliance (**Independent Person**). The Independent Person has contributed to Equifax's internal Compliance Program by providing assessment and assurance for the period 1 July 2021 to 30 June 2022 (**Reporting Period**) in respect of Equifax's systematic review and monitoring processes. This report provides the Assurance Review Committee's overall conclusions and assurance on compliance with the Code for the Reporting Period.

2. Process of Review and Reporting

2.1 Overview of the Assurance Reporting Process

Equifax has taken the following systematic approach in developing this Assurance Report:

1. Equifax Internal Compliance Program	2. Engagement of Independent Reviewer	3. Finalisation of the Assurance Report
• Commencement of the Annual Compliance Program and periodic Assurance Review Committee meetings • Implementation of the Equifax Compliance Program, incorporating Code compliance as the driving force for compliance activities for the reporting year • Completing the obligation register and confirming controls through the attestation process.	• Appointment of Independent reviewer • Communication with the Assurance Review Committee • Interviews with the Independent Reviewer Obligation Owners • Documentation/Support review along with agreed testing	• Presentation of Independent Reviewer's findings to the broader Assurance Review Committee • Deliberation on the Independent Reviewer's findings by the Committee • Addressing the Committee's concerns and developing a correction action plan • Report preparation and sign off by the Committee to be submitted

Equifax has prepared this Assurance Report through its Assurance Review Committee comprising of members with accountability and responsibility for the obligations set out in Schedule 7, as well as the Independent Person.

Process undertaken to gain assurance:

Step	**Process Description**
Step 1: Attestations	The assurance process uses Equifax's internal Compliance Program to enable periodic attestations of obligations and controls, by the Obligation and Control Owners. These were facilitated by the Compliance Officer and all results and findings were escalated to the Assurance Review Committee. All controls identified were mapped to the obligation. The accountable Obligation and Control Owners were provided with the obligations register and required to review control effectiveness and to provide reasonable assurance by way of supporting evidence.
Step 2: Independent review	The role of the Independent Person was to challenge and provide an independent perspective on the design suitability and operational effectiveness of internal controls and practices pertaining to the requirements of Schedule 7 of the Code. This was done through document reviews, interviews and testing. *Note: Documents reviewed include a selection of evidence required for the purpose of obtaining reasonable assurance. This includes, but is not limited to, policies and procedures, guidelines, monitoring and review results, complaints, registers, access rights, website content, templates and application forms.*
Step 3: Review of results	The results of both the attestation and review process were presented to the Assurance Review Committee for discussion, along with any recommendations and improvements. The Assurance Review Committee has also ensured that recommendations provided by the Independent Person have been incorporated into the Equifax Corrective Actions register for implementation.
Step 4: Assurance Report	The Assurance Report was prepared with the pragmatic and collective effort of the Assurance Review Committee with the aim of providing reasonable assurance to the OPC with respect to Equifax's compliance with the Code. This report was approved by the Assurance Review Committee and Independent Person.

2.2 Assurance Review Committee

Equifax has engaged an Assurance Review Committee to oversee the preparation of this Assurance Report. The Assurance Review Committee was comprised of members from within Equifax or its related Group members with accountability in line with the obligations set out in Schedule 7 (to enable a higher standard of reasonable assurance) and was assisted by a review and report from the Independent Person[1].

The Assurance Review Committee was comprised of the following members:

Angus Luffman (Chair)	Managing Director, New Zealand
Alana Hampton	General Manager – Enterprise Risk Management and Compliance, Australia and New Zealand
Elaine Toon	Senior Manager – Regulatory Compliance and Governance
Wayne Williamson	Vice President, Head of Security, Australia and New Zealand
Philip Bowrey	Information Security Officer
Deborah Malaghan	Head of Legal, New Zealand
Bob Sparshatt	Chief Data Officer, Australia and New Zealand
Raoul Hamilton-Smith	General Manager, Technical Delivery and CTO NZ
Teresia Lai	Head of Data Ingestion
Biswanath Dutta	Data Ingestion Lead
Paul Dunne	General Manager - Customer Services, Australia and New Zealand
Nick Foster	Head of Solutions and Marketing Services
Geoff Hawkins	Head of Risk and Business Resilience, Australia and New Zealand
Suellen Heintz	General Manager, Product Development and Customer Centred Design
Jasdeep Singh	Compliance Officer
Deanne Myers	Independent Person

The Assurance Review Committee is a valuable governance body at Equifax that facilitates robust discussion relating to Code compliance and control enhancements. The Independent Person's contribution also enhances the process for Code compliance by providing an external view on internal policies, processes and frameworks, ultimately resulting in improved compliance controls and risk mitigation.

This Assurance Report confirms that the Assurance Review Committee has facilitated the necessary level of scrutiny and discussion to provide reasonable assurance that Equifax has met all its Code requirements for the Reporting Period.

Specifically, the Assurance Review Committee has, within its scope, satisfied itself that Equifax has performed the following:

[1] The Independent Person's scope was to provide an external view on internal policies, processes and frameworks when reviewing compliance with the Code.

- Embedded a culture for Code compliance through a formal Compliance Program;
- Implemented the three lines of defence to ensure that appropriate controls are in place to confirm Code compliance;
- Reviewed and updated all applicable internal policies and process documents;
- Reviewed and updated the Code obligations register on a regular basis;
- Conducted desktop reviews of documented policies and procedures, guidelines, monitoring and review results, complaints, registers, access rights, website material, templates and application forms;
- Conducted deep dives relating to any additional question areas;
- Engaged with Control Owners to assess and test control effectiveness where required;
- Considered and recorded recommendations from the Independent Person relating to control effectiveness, in the Corrective Actions register; and
- Drafted this Assurance Report in conjunction with deliberation and review sessions.

2.3 Independent Person

Equifax again retained the services of its 2020-2021 reporting year Independent Person for this Reporting Period, reappointing Deanne Myers from INFO by Design Limited. This re-appointment has meant that Equifax has had the benefit of deeper insights and informed perspective from an Independent Person familiar with its business operations particularly regarding the focus areas identified and the additional testing performed this year.

Deanne Myers is not engaged by Equifax as an employee, director or contractor of Equifax (other than, indirectly, as specified person under the contract with INFO by Design Limited for the purposes of conducting the independent review). She has not provided any other services or consulting advice to Equifax, other than in the capacity of acting as the Independent Person.

Deanne Myers is a qualified and experience professional advisor with expertise in privacy, assurance and risk with over 20 years' of experience working with a wide range of public and private organisations and sectors in both New Zealand and United Kingdom. She is a member of the International Association of Privacy Professionals (**IAPP**) as well as a Certified Internal Auditor and member of the Institute of Internal Auditors.

Her broader privacy experience includes management and development of KPMG's privacy service line in New Zealand, development and application of the Government Chief Privacy Officer's Privacy Maturity Assessment Framework (**PMAF**), and management and delivery of methodologies for privacy maturity and risk assessments, privacy training, privacy policy and procedures, breach response design and assessment and privacy framework development.

Deanne Myers confirms her independence.

2.4 Independent Reviewer's Report Summary

The assurance process undertaken by the Independent Person during this Independent Review included:

1. Review of documentation provided by Equifax, while onsite at Equifax's Auckland office, and off-site. One hundred and eighty (180) documents were reviewed and assessed against the requirements of the Code.
2. Interviews with eighteen (18) key staff, with additional assistance provided by Equifax's Compliance Officer as required. The list of interviewees is included as Appendix 2.
3. Assessment of the policies, processes and controls identified through the review of documentation, interviews, walk-throughs and sample testing, against the requirements of the Code. This assessment included establishing whether reasonable assurance of compliance with Equifax's obligations could be determined.

4. Where evidence of compliance was not provided or opportunities for improvement were identified, a risk assessment was undertaken. This risk assessment considered the likelihood of non-compliance with Equifax's obligations under the Code. Recommendations that reflect this risk assessment were then developed.

The approach for this review differed from previous years in that areas where there had been no change since the prior year were not reviewed in detail. However, selected topics were subject to more in-depth analysis. These areas included walk-throughs, process analysis and testing of a sample of:

- Incidents reported in the Incident Reporting Tool
- Suppression requests
- Direct marketing requests (a walk-through was undertaken but compliance testing was not, due to restrictions on sharing personal information externally which meant the reviewer could not select a sample independently)
- Complaints/corrections (these are not currently differentiated in process by Equifax).

Overall, the Independent Person concluded, in relation to the Reporting Period, that there was sufficient evidence that Equifax was in compliance with the obligations of the Code relating to their:

- Policies, procedures, controls and subscriber agreements
- Monitoring of policies, procedures, controls and subscriber agreements, and
- Actions taken on deficiencies identified

One recommendation has been made to ensure Equifax can continue to demonstrate compliance with the Code:

Recommendation: The planned monitoring of compliance against the business requirement to not store personal and credit information in the cloud collaboration tools used for document storage and email (for example, Google) should be prioritised and undertaken from this year. Equifax has accepted the recommendation and this is in the process of being actioned.

The Independent Person is of the opinion that there are no indications of non-compliance with the Code or of Equifax not meeting its obligations and that Equifax is well placed to continue to be able to provide reasonable assurance over its compliance with the Code.

3. Summary of Assurances

This section contains a summary of the assurances required under the Code with a response from Equifax and the findings of the Independent Person.

3.1 Schedule 7 Section 1 Assurances

Process of review and reporting

Section 1	Expectation per the Code	Equifax Assurance response
(a)	The report must include a summary of the systematic review process and the methodology followed by the reviewer.	Refer to section 2.1 of this Assurance Report which outlines the assurance and review process and methodology followed by Equifax. The Independent Person's review process is outlined in section 2.4 of this Assurance Report.
(b)	The report must include a statement identifying the members of the review committee, including the independent person.	Refer to section 2.2 of this Assurance Report which identifies the members of the review committee along with the Independent Person from INFO by Design Limited.
(c)	The report must include a statement from the Independent Person confirming their independence, summarising their expertise and outlining their involvement with the assurance process and preparation of the report.	Refer to section 2.3 of this Assurance Report which notes a confirmation from the Independent Person confirming their independence as well as a summary of their expertise. Refer to section 2.1 outlining the assurance process including the involvement of the Independent Person. Further elaboration has been included from the Independent Person in section 2.4.
(d)	The report must include a confirmation that the independent person is not an employee, director, or owner of the credit reporter.	Refer to section 2.3 of this Assurance Report which includes a statement noting that the Independent Person is not an employee, director or owner of the credit reporter.

3.2 Schedule 7 Section 2 Assurances

Assurances relating to policies, procedures, controls and subscriber agreements

Section 2	Expectation per the Code	Findings of the Independent Person and Equifax
(a)	In relation to the applicable period, Equifax had policies in place that give effect to the requirements of the Code.	Equifax has a comprehensive suite of policies at a global and regional level. These policies give effect to the requirements of the Code. Compliance with these policies and associated procedural documents is mandatory. Equifax has created an obligations register which is mapped to the controls register. This is used for identifying owners of the controls that support compliance with the Code, including policies. The registers clearly and comprehensively identify the policies in place for each requirement of the Code. The Privacy Policy was updated and is available via Equifax's website. It is comprehensive and provides the appropriate information for our consumers.
(b)	In relation to the applicable period, Equifax had policies in place to ensure that any arrangement with a related company accords with clause 4(2) of this Code.	Equifax had policies in place to ensure that any arrangements with related companies accord with clause 4(2) of the Code. All policies are clearly identified as being either A/NZ or New Zealand-specific or being Global in application. Company-specific policies may also be created if there is a regulatory reason to differ from group-wide policies; however, these require review and approval prior to being implemented.

(c)	In relation to the applicable period, Equifax had internal procedures and controls in place to give effect to the policies and requirements of the Code.	Equifax has internal procedures and controls in place to give effect to the policies and requirements of the Code. The policies are supported by detailed process and guidance documentation. Responsibilities for policies (development, compliance, and monitoring) are well understood. Compliance is supported by organisation-wide and team-based training, including at onboarding. Compliance with policies and procedural documentation is mandatory and monitored through a variety of means: ● First line oversight and review; ● Second line management oversight (risk framework, quality assurance monitoring); and, ● Third line (internal audit and this independent review). There is an attestation process whereby obligation and control owners report on the procedures and controls implemented to give effect to the policies and requirements of the Code. Processes for identifying, reporting and monitoring non-compliance are embedded throughout the business and include data monitoring and ongoing testing. The following mechanisms continue to be enhanced: ● Training has been reviewed and updated ● Tools for reporting incidents and raising compliance queries has been enhanced ● Enhanced compliance oversight as a result of the obligations register which allows more comprehensive and detailed information on the existence and effectiveness of controls ● Increase in compliance testing Lastly, a Privacy Impact Assessment (PIA) is undertaken for all changes.

(d)	In relation to the applicable period, Equifax had appropriate procedures in place to ensure that any information requested under Rule 6 is received only by that individual or, where the request is made by an agent on behalf of that individual, only by that individual or his or her agent.	Equifax's processes for access requests include verification of the identity of individuals, confirmation of contact details, requirements for privacy waivers from third parties and secure sending of information (for example, passwords are required to open credit reports, PINs are required to action Suppression requests). Documentation (both for internal use and for individuals to understand their rights) is comprehensive and well understood. Procedures to avoid bundling of authorisations that may circumvent the code's prohibition on marketing and direct marketing include: ● Use of privacy impact assessments for all new use and changes to existing use requests ● There is a separation of the Marketing database from the Bureau with restrictions on access ● The terms and conditions in the subscriber agreement explicitly prohibit use for marketing ● System rejection of bundled requests. Internal processes to ensure these are actioned appropriately are also comprehensive and well understood, with results being reported, and compliance with it monitored.

(e)	In relation to the applicable period, Equifax provided information and training to its staff to ensure compliance with the policies, procedures and controls.	Equifax provides information and training to its staff to ensure compliance with the policies, procedures and controls. In addition to the information provided to staff via Equifax's policies and procedures, training is delivered to staff and contractors to ensure compliance with the policies, procedures and controls. This includes both online training modules and training delivered to specific teams. Training has been reviewed, updated and rolled out during the last year on Privacy, Risk and 'how to' training on incident reporting and queries to Compliance. 'High Risk User' training has also been developed and delivered to reduce the risk associated with the move to Google Drive. The content is appropriate in terms of the Code and Equifax's policies, procedures and controls. Content is targeted at appropriate areas (i.e. Privacy Impact Assessments, Compliance, Privacy 101, Credit Reporting). Completion of training is monitored and non-completion or ongoing lack of assessed understanding is escalated to management for resolution.
(f)	In relation to the applicable period, Equifax ensured that subscriber agreements that complied with Schedule 3 were in place before disclosing credit information.	Equifax executes subscriber agreements that complied with Schedule 3 with its subscribers before disclosing credit information. The Operations team do not provide access to Equifax's systems until an agreement is executed, and the subscriber has met the on-boarding requirements.
(g)	In relation to the applicable period, Equifax ensured that access arrangements under Schedule 4 were in place before disclosing credit information.	Equifax's systems do not allow disclosure until an agreement has been approved and the subscriber has met the on-boarding requirements. The agreement requires consent from individuals applying to join the intelligence and security agency. Equifax disguises the footprint from being shown on the customer's credit file, preventing the footprint of the agency being shown.

3.3 Schedule 7 Section 3 Assurances

Assurances relating to monitoring of policies, procedures, controls and subscriber agreements

Section 3	Expectation per the Code	Findings of the Independent Person and Equifax
(a)	In relation to the applicable period, Equifax undertook monitoring activities to ensure reasonable compliance with the code, including that Equifax followed its own policies, procedures and controls.	During this Reporting Period, Equifax undertook the following assurance activities: quality assurance monitoring with an increase in compliance reviews, internal audit, risk management processes, breach and incident reporting, support from the Compliance team in case of queries or issues, increase in the quantity and scope of privacy impact assessments and an enhancement in the communication on obligations and related controls owned by management. As noted above, there is an extensive set of policies and procedures for staff to follow when undertaking any activity related to the Code. These documents are comprehensive and are supported by training. Incidents (including CRPC-related incidents) are tracked through the Compliance Incidents Register. Corrective actions are documented within the Corrective Actions Register. Privacy impact assessments are a key part of Equifax's means of ensuring compliance with the Code, the Privacy Act and 'good practice'. PIAs are undertaken for new data sources/acquisitions, and changes to systems/platforms and processes/product usage. The second line activities put in place by Equifax rely on oversight and review by management. The obligations and controls register, and documentation of policies and Standards, are used to ensure that management is aware of their responsibilities, including their responsibilities to obtain assurance on the effectiveness of the controls in place. Resourcing of the compliance team in NZ means that there are limits on the quantity of additional compliance checking that may be carried out in relation to this. Equifax therefore designs its annual plans based on an internal assessment of risk, as is appropriate for our three lines of defence model.

(b)	In relation to the applicable period, Equifax undertook monitoring activities to ensure reasonable compliance with the code, including that the information held by Equifax was protected by reasonable security safeguards.	During the period, the information held by Equifax was protected by reasonable security safeguards. There is a comprehensive security framework in place including risk assessment and response during design, and both external and internal monitoring, testing and response.
(c)	In relation to the applicable period, Equifax undertook monitoring activities to ensure reasonable compliance with the code, including that Equifax processed information privacy requests in accordance with rules 6 and 7.	Equifax undertook monitoring activities to ensure reasonable compliance with the Code, including that Equifax processed information privacy requests in accordance with rules 6 and 7. Documentation (both for internal use and for individuals to understand their rights) is comprehensive and well understood. Internal processes to ensure these are actioned appropriately are also comprehensive and well understood, with results being reported, and compliance with it monitored.
(d)	In relation to the applicable period, Equifax undertook monitoring activities to ensure reasonable compliance with the code, including that Equifax took such measures as were reasonably practicable to avoid the incorrect matching of information held by Equifax.	Equifax undertook monitoring activities in relation to the incorrect matching of information. Equifax applies matching criteria for both manual and automated matching. There is comprehensive documentation and guidance for users, and detailed processes. Matching accuracy and control is reported regularly to governance committees. Root cause analysis of specific cases of incorrect matching is undertaken and informs matching criteria and process. Analysis of data relating to accuracy (including matching accuracy) is undertaken monthly and shows this is improving over time. Specific concerns are appropriately escalated. Equifax is currently working to improve its data matching as part of its technology and business transformation efforts.

(e)	In relation to the applicable period, Equifax undertook monitoring activities to ensure reasonable compliance with the code, including that the information held by Equifax was subject to reasonable checks to ensure that it was accurate, up to date, complete, relevant and not misleading.	Equifax undertook monitoring activities to ensure that the information it held was accurate, up to date, complete, relevant and not misleading. Checks to ensure accuracy are built into the change management process, including the privacy impact assessment process. Requirements for quality, accuracy, completeness and timeliness of data provided to Equifax are included in subscriber agreements and ensured by checks run over data before it is imported. Data analysis is undertaken regularly. The criteria include compliance with specified values (which include accuracy and timeliness). Results of the analysis are reported monthly and show trends and changes over time. Accuracy is shown to be improving continually. Our monthly Data Quality Reports cover a wide range of data analytics and results over data matching and changes in enquiries and results over time. These are widely distributed and are primarily used to identify any anomalies or change, which is then investigated. The Independent Person noted that Equifax undertook appropriate monitoring activities to ensure reasonable compliance with the code, including that the information held by Equifax was subject to reasonable checks to ensure that it was accurate, up to date, complete, relevant and not misleading. However, two instances were observed; it is to be noted that appropriate remediation actions had been taken in relation to the instances: ● a missing result in the Data Quality reports for a specific piece of information. Equifax is in the process of implementing enhancements in our Data Quality reports. At the time if the review, the enhancements were yet to be implemented hence the missing result ● an incident investigated under the Regulatory Incident Reporting Tool noted that an issue with data information received was not identified due to a high rejection rate. This was remediated with more focused monitoring and a lowering of the rejection rate to be investigated.

(f)	In relation to the applicable period, Equifax undertook monitoring activities to ensure reasonable compliance with the code, including that Equifax's reporting and retention of credit information was in accordance with Rule 9 *(Retention of credit information)* and Schedule 1 *(Maximum reporting periods).*	The retention requirements have been documented for internal Equifax use. The data team reviews compliance with specified criteria, including retention periods. Much of this is automated, with manual checks also applied. Retention periods are embedded in the systems, and there is no ability for staff to override these. It is noted that Equifax has implemented a business requirement to not store personal information and credit information in cloud collaboration tools used for document storage and email. Employee guidance and training about this requirement has been rolled out to all individuals who have access to personal information and/or credit information to perform duties associated with their role. Further controls are also in development to support this, including a monitoring process. Despite this, Equifax has been working with its third party vendor to ensure appropriate retention rules are implemented across all cloud collaboration tools as an additional measure.
(g)	In relation to the applicable period, Equifax undertook monitoring activities to ensure reasonable compliance with the code, including that Equifax processed direct marketing lists in accordance with Schedule 10	Equifax monitored the processing of direct marketing lists appropriately. Controls are in place to ensure that requests are only processed when received from approved subscribers. These are processed only when set criteria are met. Compliance is monitored, and the requirements are explicitly communicated to subscribers. These controls include training and guidance, automated checking and automated processing. Equifax takes a risk averse approach to processing of direct marketing lists in accordance with Schedule 10, including "if in doubt, leave it out".

(h)	In relation to the applicable period, Equifax undertook monitoring activities to ensure reasonable compliance with the code, including that Equifax processed suppression, release or cancellation requests in accordance with Schedule 8.	There is a process description and a suppression request policy in place which outlines the following: ● Process for granting suppressions ● Process for termination/cancellation of suppressions ● Embedding a temporary release policy process. ● PIN verification and ID verification processes The Independent Person performed a walkthrough and testing of the processes applied for a sample of suppression requests. It was found that the process was followed in all cases in the sample, with one minor exception noted: One of the requests had an incorrect status indicating that it had been processed by the bot rather than manually. The Independent Person has been assured that this does not impact on the service provided to the consumer or to their data but impacts only on internal workflow reporting. Automated and manual compliance checking is undertaken on a regular basis. Equifax has an agreement in place with the other credit reporters, per Schedule 8 (1.2).
(i)	In relation to the applicable period, Equifax undertook monitoring activities to ensure reasonable compliance with the code, including that Equifax processed complaints in accordance with Clause 7.	Equifax processes complaints in accordance with Clause 7 of the Code, and: ● Responsibilities for dealing with complaints are clear and well understood; ● The Complaints Procedure is documented and consistent with all the requirements of clause 7; and ● The Summary of Rights is made available to complainants and is on Equifax's website. Complaints are recorded and progress in resolving them is tracked via the online Incident Reporting tool. This tool provides clear and comprehensive information on complaints received with links to related documentation and correspondence, steps taken to manage the complaint and means by which it was resolved. Compliance is monitored through an attestation process and reporting. Processes for identifying, reporting and monitoring non-compliance are embedded throughout the organisation.

(j)	In relation to the applicable period, Equifax undertook monitoring activities to ensure reasonable compliance with the code, including that Equifax's website displayed accurate information that gave effect to rules 6(7)(b), 7(5)(b) and clause 8.1 of Schedule 8.	Equifax's website displays accurate information consistent with Code requirements.
(k)	In relation to the applicable period, Equifax undertook monitoring activities to ensure reasonable compliance with the code, including that subscribers complied with agreements and controls.	Equifax undertook appropriate monitoring activities to ensure reasonable compliance with the Code, including to ensure that subscribers complied with agreements and controls. Subscriber obligations, including the obligation to cooperate with Equifax's monitoring requirements, are made clear to subscribers. Equifax has implemented automated and ad hoc monitoring of compliance and responds to identified non-compliance (including suspension of subscriber accounts where appropriate). Equifax performed a subscriber audit review this year which covered the following areas: consent requirements; purpose code matching to subscriber requirements; and subscribers did not perform checks on themselves. Equifax has subsequently developed areas of scope for inclusion in the next upcoming reviews, including confirmation and review of the subscriber form/contract and any further areas noted by the Independent Reviewer.
(l)	In relation to the applicable period, Equifax undertook monitoring activities to ensure reasonable compliance with the code, including that the intelligence and security agencies complied with any access arrangements and controls.	The management attestation process covers this agreement and it has also been reviewed by Internal Audit. The SIS is subject to review as part of the scheduled subscriber audits as well those which are undertaken by the Compliance team.

(m)	In relation to the applicable period, Equifax undertook monitoring activities to ensure reasonable compliance with the code, including that the requirements on both the subscribers and the credit reporter under Schedule 10 in relation to tracing individuals were met.	This is actioned through a standard contract. Activities to ensure compliance are completed in a number of ways, including pre-screening, specific T&Cs for subscribers, the completion of privacy impact assessments for any newly acquired datasets, and the suppression process automatically flows through Equifax systems to prevent inconsistencies.

3.4 Schedule 7 Section 4 Assurances

Assurances relating to an action taken on deficiencies identified

Section 4	Expectation per the Code	Findings of the Independent Person and Equifax
(a)	In relation to the applicable period, where, during its systematic reviews, monitoring activities or as a result of a complaint, Equifax identified a breach of an agreement, policy, procedures, control, or requirement of the code, Equifax investigated that breach and, where appropriate, took prompt remedial action.	Where Equifax identified a potential breach of an agreement, policy, procedures, control, or requirement of the code, Equifax investigated the matter and, where appropriate, took prompt remedial action. A corrective actions register is used by Compliance to track breaches, incidents and progress made on recommendations made as a result of audit, review or investigation. This is supported by a defined Data Breach Policy and Response Plan and supporting processes. The Incident Reporting Tool has been enhanced and made widely available, as well as requiring comprehensive detail. Instructions and procedures for reporting are being developed. Responsibilities in relation to breaches and complaints are known and understood, and responsibilities, processes and reporting are comprehensively documented.
(b)	In relation to the applicable period, where a deficiency was identified in the previous year's report, Equifax, where appropriate, took prompt remedial action.	No deficiencies were identified in the previous year's report. The outstanding recommendation from 2020/21 review regarding the finalisation of the draft Privacy Policy has been actioned.

4. Additional Questions

The following additional questions were raised as areas of interest by the Commissioner. Equifax's responses are set out below:

Note: INFO by Design had completed their review when the additional questions were received. Based on their review, they have thus provided comments where they were able to. The OPC confirmed that the Independent Person is not required to comment on the additional questions.

OPC Additional Info Request	Equifax Response	Independent Person comment
Mandatory privacy breach notifications There were low volumes of privacy breach notifications and privacy complaints made to the Office of the Privacy Commissioner during the 2021-2022 financial year. What policies and procedures or self-assessment tool do you have in place to assure the Commissioner of complaints made to your agency (or near-misses identified by your agency) and bring correctly triaged? How can the Commissioner be satisfied our Office is being advised if breaches that should be brough to our attention?	Equifax has an online tool within Service Now* which is known as the Governance, Risk & Compliance Incident Reporting tool with the purpose of capturing and notification to Compliance of any compliance incidents. This provides for electronic completion of incident reports and the management of the process flow. All reporting relating to compliance incidents or breaches is now generated through the tool which also acts as a register. The Tool also provides for the assignment of incidents to fraud and security teams for parallel investigations and to Legal in instances where a disclosure is needed to be made to the appropriate Regulator. The tool provides a section to outline an assessment of the incident including severity, whether a breach has taken place, whether it needs to be reported to the regulator, as well as corrective actions to be taken. The tool is subject to ongoing phased enhancements and improvements in functionality. Training on the making of submissions through the online tool has been provided to all NZ staff. Broadcasts were and are released as and when necessary to complement the tool and its existence and uses. On a quarterly basis, the incidents and corrective actions	The Independent Person reviewed Equifax's processes for investigating and responding to reported or identified breaches and complaints. This included: 1. Review of the policies and documented processes for identifying, managing and reporting/escalating breaches and complaints 2. Review of the tool used for recording and managing breaches and complaints 3. A walk-through of the actions taken in response to a sample of items recorded in the tool. The Independent Person concluded that where, during its systematic reviews, monitoring activities or as a result of a complaint, the credit reporter identified a breach of an agreement, policy, procedures, control, or requirement of the code, Equifax investigated that breach and, where appropriate, took prompt remedial action. Based on review of the corrective actions register and interviews with the Compliance team no complaints or near misses were reported to the Office of the Privacy Commissioner in the period.

	are reported to the Risk, Compliance and Security Committee as part of the reporting pack. * ServiceNow is a digital workflow platform utilised by Equifax in managing its incidents, corrections and complaints workflow and processes.	
Transferring of information to other business channels within the agency Credit reporting agencies have a variety of business functions. What assurances and measures are put in place to ensure personal information is shared within the appropriate business channel and to only shared to third parties for a lawful purpose and kept secure?	Equifax has in place a Privacy Impact Assessment Policy and Process through which Equifax can manage, review and approve where personal information is being shared appropriately between business channels and third parties. The Privacy Impact Assessment (PIA) is a systematic assessment of a project that looks at the sourcing, use and sharing of personal information. The PIA identifies the impact that the project might have on the privacy of individuals and sets out recommendations for managing, minimising or eliminating the impact. Where there is a new or updated initiative including the use of information in a different way, a PIA is completed or an existing PIA is updated and reviewed again. Approval for a PIA is required from the Compliance team as well as Data Governance and Legal where required. There are three types of PIA templates: ● Data Source PIA ● Data Use PIA ● Platform PIA All PIA's have a section that requires the business to explain and note where the information is being shared i.e. which business channels the information travels through and the involvement of any third parties. These	The Independent Person: 1. Confirmed that appropriate policies, documentation and training are in place to ensure personal information is shared within the appropriate business channel and to only shared to third parties for a lawful purpose and kept secure 2. Confirmed awareness of policy requirements of persons interviewed during the Review 3. Reviewed Equifax's existing and planned global and New Zealand security arrangements (at a high level – note that a full technical security review was not undertaken) 4. Confirmed access restrictions in the systems for which testing was undertaken during the review 5. Confirmed that compliance testing of subscriber agreements, including disclosure, was not undertaken by Equifax this year. The Independent Person has recommended that the scope of subscriber audits be widened, to focus on all relevant areas of compliance with the agreements and the Code. 6. Reviewed the subscriber agreement template and confirmed that subscribers agree to comply with the relevant aspects of the Code.

	are appropriately assessed within the PIA to ensure the business is lawful in its purpose and the information is kept secure.	
The use of credit reporting agency databases (or third-party agencies) to obtain personal information Landlords can search prospective tenants on a third-party or credit reporting agency owned database. In the case of landlords using a credit reporting agency owned database (or via a third-party agency) how long is that pooled personal information retained for by the agency, and how is this explained to tenants so they know they have the right to access and change their information if need be? How is that information protected and only the correct people get to view it?	Note: Equifax assumed the OPC is referring to information that is available for the Landlord to access and the retention of that information by Equifax. <u>Retention of information</u> Personal information is retained by Equifax until we have use of it within our Bureau. Credit information on an individual is retained in line with the maximum reporting periods provided in Schedule 1 of the Credit Reporting Privacy Code 2020. No Comprehensive Credit Reporting information is provided in response to a landlord request. <u>Privacy policy</u> Equifax has a privacy policy which is published online on the Equifax website which notes what information is collected and how. The policy also notes when we disclose information to prospective landlords. There is also a section on how one can access or correct one's information. <u>Protection of information</u> In order to access an Equifax product, subscribers have to complete a Subscriber Application Form which has to be reviewed and approved by Equifax. By completing, signing and submitting the Subscriber Application Form, the subscriber confirms their acceptance of Equifax's Terms of Supply. Equifax's standard Terms of Supply include	This was not reviewed by the Independent Person.

	requirements for subscribers to have the relevant processes, procedures and systems in place to ensure the credit reporting information is accurate, up-to-date and complete, and sufficiently protected which are in line with Schedule 4 requirements around Access agreements. Once an agreement has been signed and they become a subscriber, they are assigned an access purpose code which is determined from the purpose i.e. Landlords are given a specific access purpose code which ensures that they do not have access to CCR information. They are also provided separate login details.	
Tracing individuals for unclaimed monies The Office of the Privacy Commissioner wishes to ensure all credit reporting agencies are following Schedule 11 of the Code correctly. While the Office acknowledges this question was asking in the 2019 assurance year, at that stage this provision was very new and it had not yet been used. Now three years later we wish to seek assurances around how agencies are using the credit reporting system for tracing to facilitate the return of money owed to individuals. Have you experienced any system issues or concerns from individuals and if so, please provide information around this and what is being done to mitigate these issues?	Prior to accepting or processing any data, a Statement of Work is completed. An eTrace batch input data layout is provided to ensure data is supplied in the required format which is supplied via a secure link. The eTrace product matches consumers against the data held in Equifax bureau and when a suitable match is found, returns the applicable data we hold. We ensure that the template communication is provided to the customer and is in line with the requirements of the Schedule. Equifax will match the supplied name and address, and the eTrace updated address to the Marketing Association Deceased Register using a very tight match. Equifax will also run the eTrace appended addresses through an Address Cleanse process, whereby addresses are corrected, where necessary. The customer's nominated mail house will perform a merge of the letter	Equifax's documented requirements, templates and processes for tracing were reviewed. The Independent Person concluded that there is reasonable assurance that the requirements under Schedule 11 in relation to tracing individuals were met. The Independent Person cannot comment however on system issues or concerns from individuals during the period reviewed as this was not included in the scope of testing undertaken during the review.

	template with the eTrace results provided by Equifax and provide a sample of these letters for Equifax for review on behalf of the customer. For clarity, at no time will the customer be provided with copies of the merged letters as this contravenes the requirements of Schedule 11 of the Code. Till date we have not experienced any system errors or concerns from individuals.	
Role of Independent Reviewer The role of the independent reviewer is to ensure that these checks are robust and have picked up any non-compliance. The assurance reporting should therefore note any issues that have arisen through the year and how they have been addressed or resolved. It would be a disappointing situation to have an independent reviewer find no issues only to have the Commissioner or this Office consider exercising other powers or functions should there be a repeat of non-compliance. As mentioned under clause 9(3)(c) of the Code we therefore request that all credit reporters speak with their independent reviewer and emphasise that they are an independent person, who is required to question/test systems, processes and practices and independently review these against the requirements of the Code.	Equifax has passed on this requirement to INFO by Design, emphasising the need for and importance of the independence of the reviewer.	Deanne is not an employee, director or contractor of Equifax. Nor has she provided any other services or consulting advice to Equifax other than as the independent person – a role she has filled for the last three independent reports. The Independent Person has sought sufficient information to inform a conclusion that there is reasonable assurance that Equifax complies with the Credit Reporting Privacy Code. The review consisted of assessment of the policies, processes and controls identified through the review of documentation, interviews, walk-throughs and sample testing, against the requirements of the Code. Selected topics were subject to more in-depth analysis. These areas included walk-throughs, process analysis and testing of a sample of: ● Incidents reported in the Incident Reporting Tool ● Suppression requests

		• Direct marketing requests (a walk-through was undertaken but compliance testing was not, due to restrictions on sharing personal information externally which meant the reviewer could not select a sample independently) • Complaints/corrections.