Equifax New Zealand Information Services and Solutions Limited

Assurance Report

Year ending 30 June 2024

Table of Contents

1. Introduction

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

1.2 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.

1.3 Clause 8 of the Credit Reporting Privacy Code 2020 (**Code**) mandates that Equifax provide an annual report (this **Assurance Report**) to the Office of the Privacy Commissioner (**OPC**) prepared in accordance with the requirements of Schedule 7 of the Code. Equifax has endeavoured to address all the requirements of the OPC Assurance Review through this Assurance Report.

1.4 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, 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 2023 to 30 June 2024 (**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

Overview of the Assurance Reporting Process

2.1 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 obligations register and confirming controls through the attestation process.	• Appointment of Independent Person. • Communication with the Assurance Review Committee. • Interviews with the obligation owners and control owners. • Documentation/Support review along with agreed testing.	• Presentation of Independent Person's findings to the broader Assurance Review Committee. • Deliberation on the Independent Person's findings by the Assurance Review Committee. • Addressing the Assurance Review Committee's concerns and developing a correction action plan, where required. • Report preparation and sign off by the Committee for submission.

2.2 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.

2.3 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 Senior Manager – Regulatory Compliance and Governance 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, if any, 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.

Assurance Review Committee

2.4 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].

2.5 The Assurance Review Committee was comprised of the following members:

Lisa Postlewaight	Country Manager, New Zealand
Alana Hampton	GM – Enterprise Risk Management and Compliance, Australia and New Zealand
Wayne Williamson	Chief Information Security Officer - Australia, New Zealand and Emerging Markets
Deborah Malaghan	Head of Legal, New Zealand
Paul Dunne	GM - Customer Services, Australia and New Zealand
Geoff Hawkins	Head of Risk and Business Resilience, Australia and New Zealand
Elaine Toon	Senior Manager - Regulatory Compliance & Governance
Marcus Bruhn	GM, Data Commercialisation & Governance
David VanderStraaten	Segment Leader
Michelle Olbricht	Independent Person

2.6 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.

2.7 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.

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

- 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.

Independent Person

2.9 Equifax retained the services of Michelle Olbricht, a consultant from INFO by Design Limited as its Independent Person for this Reporting Period.

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

2.10 Michelle Olbricht 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.

2.11 Michelle is an experienced professional advisor with expertise in privacy, compliance, and operational risk. She has over 20 years of experience working with a wide range of public and private organisations and sectors in New Zealand. In particular, she has several years of experience in operations management and compliance within the financial services industry. Michelle has also held the role of Privacy Officer for two organisations.

2.12 Before joining INFO by Design, Michelle was a senior manager at KPMG New Zealand. She was responsible for providing advice and guidance to a wide range of public and private sector organisations to assist them with improving privacy and compliance practices.

2.13 Michelle has a Bachelor of Laws from Victoria University of Wellington.

2.14 Michelle Olbricht confirms her independence.

Independent Person's Report Summary

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

- Review of documentation provided by Equifax, while onsite at Equifax's Auckland office, and off-site. Two hundred and twenty (220) documents were reviewed and assessed against the requirements of the Code.
- Interviews with fourteen (14) key staff.
- 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.
- 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.

2.16 This year, walk-throughs and process analyses were also conducted for access requests and requests for corrections/complaints. The complaints process is combined with the corrections process. As a result, walk-throughs of a sample of corrections ensured that the correction was managed within appropriate timeframes and in accordance with the corrections processes. This year, the OPC did not provide additional topics for review.

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

2.18 The Independent Person concluded that, in relation to the Reporting Period, there was sufficient evidence that Equifax complied with the obligations of the Code relating to the following:

Policies, procedures, controls and subscriber agreements

2.18.1 Equifax has a comprehensive suite of documented policies, procedures and controls that give effect to the requirements of the Code. A continuing review cycle is in place for all policies, procedures and controls. Ownership of these is clear, and requirements are well understood by all staff.

2.18.2 There is comprehensive induction and ongoing training and awareness activity both at an enterprise level and at business unit level. This training ensures that staff understand the requirements of the Code as they relate to their roles and responsibilities.

2.18.3 There are processes and system controls in place to ensure that subscriber agreements are in place before credit information is disclosed.

Monitoring of policies, procedures, controls, and subscriber agreements

2.18.4 Equifax's internal assurance processes are based on the three lines of defence, in line with accepted good practice.

2.18.5 At the first line of defence, there is communication and ownership of obligations and controls relating to the Code's requirements. This is supported by comprehensive instructions for all activities and services related to the Code, including training modules and extensive policy and process documentation. Privacy impact assessments are a key part of Equifax's means of ensuring compliance with the Code, the Privacy Act and 'good practice'. The process is accepted by management as a necessary part of managing risk and is implemented across relevant areas.

2.18.6 Equifax has a comprehensive Quality Assurance evaluation program focused on assessing high-risk activities, including activities undertaken by new starters, new and amended processes, activities related to audit outcomes, and customer feedback. The Quality Assurance team closely collaborates with the Customer Service Team, which engages in ongoing manager/team leader monitoring activities.

2.18.7 Equifax places a strong emphasis on continuous improvement. Whenever potential or actual issues are identified, the focus is on pinpointing the root cause and implementing solutions to resolve them. Examples include efforts to improve the processing of mixed files for twins and data ingestion activities.

2.18.8 In the 2022-2023 report, it was noted that due to resource issues, Equifax was unable to carry out control monitoring and testing activities as planned. To address this, Equifax hired a Compliance Manager for New Zealand in April 2024. This manager plays a key role in conducting control testing and monitoring activities in the New Zealand environment. Throughout the reporting year, Equifax has been able to conduct control testing and monitoring activities, particularly in the higher-risk areas of subscriber activities. Additional high-risk activities are scheduled for review in the second half of 2024, including complaints and corrections reviews. The Control Testing and Monitoring Team is also implementing a new tool to improve the efficiency of monitoring activities.

Actions taken on deficiencies identified

2.18.9 Last year the independent reviewer recommended that Equifax should identify and implement strategies for increasing second-line monitoring activities to ensure that it is satisfied that it follows its policies, procedures, and controls, particularly for higher risk areas of the Code. As noted above, these monitoring activities were undertaken by the newly appointed Compliance Manager.

2.18.10 Over the period where Equifax has identified a breach or issue, it has taken prompt action on investigating and remediating that breach or issue. There are several mechanisms in place to identify and manage these.

2.18.11 Equifax has addressed the two recommendations and one opportunity for improvement identified in last year's report. It has promptly resolved issues with the website when they were raised. Additionally, progress has been made with the control monitoring and testing program.

2.18.12 In addition, Equifax reviewed its incident reporting processes after an opportunity for improvement was identified. This related to resolved customer service complaints. New reporting requirements

were implemented on 1 May 2024. The Compliance Team is collaborating with the Customer Service Team to collect and act on feedback to improve the process around this new reporting requirement.

3. Summary of Assurances

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

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 paragraphs 2.1 to 2.3 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 paragraph 2.15 of this Assurance Report.
(b)	The report must include a statement identifying the members of the review committee, including the independent person.	Refer to paragraph 2.5 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 paragraphs 2.9 to 2.14 of this Assurance Report which notes a confirmation from the Independent Person confirming their independence, a summary of their expertise, as well as outlining the assurance process including the involvement of the Independent Person.
(d)	The report must include a confirmation that the independent person is not an employee, director, or owner of the credit reporter.	Refer to paragraph 2.10 of this Assurance Report which notes that the Independent Person is not an employee, director, or owner of the credit reporter.

Schedule 7 Section 2 Assurances

3.2 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 (Australia and/or New Zealand) level. These documents give effect to the requirements of the Code. Ownership of policies is well understood and is documented in the Obligations Register. Obligation and control owners regularly attest to the currency of processes or controls or confirm changes to processes or controls. Oversight of Equifax's policy framework is delegated to the Risk, Compliance & Security Committee (**RCSC**) Policy Sub-Committee, which has oversight of the Policy Review Schedule, and reviews and approves updates to relevant local policies.
(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.	There are no changes from last year's report. There are five New Zealand entities, four of which are holding companies. Equifax New Zealand Information Services and Solutions Limited is the operating entity. As noted above, Equifax has a framework that applies both global policies and policies at a regional (Australia and/or New Zealand) level. The policy framework applies to all entities for Equifax in the region.

(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. Internal procedures and controls include: • A privacy compliance program to oversee compliance with obligations and requirements. This program is used across the region but has a focus on Australian obligations. A New Zealand version of the compliance program is planned for 2024-2025. • Ownership of obligations and controls is assigned, and the Compliance function undertakes an attestation process quarterly. • A range of process and procedure documentation for functions across Equifax for New Zealand-related functions. • Organisation-wide onboarding and annual training. Team-specific training is also provided at regular intervals. Additional training for Equifax employees and subscribers when issues are identified. • First-line quality assurance reviews, peer reviews and manager oversight. Second-line monitoring and testing program. Third-line audit program. • System controls and checks. Error messages are produced, investigated, and resolved. • A wide range of global security controls. • Incident management procedure and system for recording incidents and breaches, with oversight of corrective actions. • Update of processes and controls where issues or areas of improvement are identified. Equifax provided examples where this has happened during the period, including improvements in the bulk deletions process and ingestion processes.

(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 the individual, only by that individual or their agent; such procedures must amongst other things ensure, as far as possible, that where information intended for an individual is received by a properly authorised agent that it is not subject to bundled authorisations for other purposes that would have the purpose or effect of circumventing the Code's prohibitions on marketing and direct marketing;	Equifax has comprehensive procedures in place for responding to access requests as required by Rule 6. Written procedures are comprehensive. The Customer Services team members are provided comprehensive on-the-job training and ongoing support. Procedures and controls include: • Verification of identity and contact details. • Third-party waiver process. • Automated processes via RPA (robot), which verifies requirements and sends automated credit reports. Error messages are investigated and resolved. • Credit reports are encrypted, and a separate email is sent to the requestor with a password. Procedures to avoid bundling of authorisations include: • When a consumer provides their personal information for the purpose of requesting their own credit file, that information can only be used to update their credit file if specific consent is given. This consent cannot be bundled with any other services. • Use of privacy impact assessments for all new use requests. • Internal review of multiple requests. • System rejection of bundled requests.

(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 provided information and training to its staff to ensure compliance with the policies, procedures and controls. Information and training provided to Equifax staff includes: • Mandatory onboarding training for all staff and contractors, including Privacy 101 and Credit Reporting 101. Compliance 101 is also provided, providing a general overview of compliance concepts and obligations. • Training records are maintained, and non-completion is escalated. • Annual mandatory global compliance training window in September / October each year with a nominated topic for refresh. For New Zealand, this is Credit Reporting 101, and the last refresh was completed in October 2023. • Other online training is also refreshed regularly. • Specific training is provided at business unit level. Consumer Bureau Operations Training encompasses on-the-job training, coaching, and, where required, performance management. There is a suite of training materials and weekly meetings where staff can discuss issues. • Other resources include the Privacy Toolkit intranet page and regular broadcasts/emails to staff. • Equifax utilised Privacy Week in May 2024 to conduct privacy-specific activities. This involved providing a refresher of Privacy 101 for all staff and organizing a series of activities, including quizzes, daily email broadcasts, and information on topics of interest such as the draft biometric Code of practice, as well as discussions on the future of artificial intelligence.
(f)	In relation to the applicable period, Equifax ensured that subscriber agreements that complied with Schedule 3 were in place before disclosing credit information.	There is evidence that subscriber agreements that complied with Schedule 3 were in place before disclosing credit information. Equifax's subscriber onboarding policy, process and systems do not allow subscribers access to credit information without meeting set criteria. • The Equifax NZ Bureau Subscription Policy outlines criteria for onboarding subscribers, including defining the requirements for an organisation to gain or be refused access to the NZ Credit Bureau.

		• The Equifax NZ Subscription Process Document provides detailed steps for onboarding, including key approval guidelines. • The Onboarding Leader reviews and approves/declines all new subscribers based on set criteria. • System controls are in place to ensure that this requirement is met.
(g)	In relation to the applicable period, Equifax ensured that access arrangements under Schedule 4 were in place before disclosing credit information.	There is evidence that Equifax ensured that access arrangements under Schedule 4 were in place before disclosing credit information. Equifax's subscriber onboarding policy, process, and systems do not permit access to credit information without meeting specific criteria. The intelligence community is also required to meet the same criteria as other subscribers, including obtaining consent from individuals who apply to join the intelligence and security agency. The only difference is that the agency's footprint is not displayed.

Schedule 7 Section 3 Assurances

3.3 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.	Equifax has several ways of undertaking monitoring activities to ensure that it complies with its own policies, procedures, and controls. These include: • Manager and Team Leader oversight and peer reviews • Quality Assurance Evaluations are focused on process changes and where issues were observed during previous quality assurance activities. Where errors were addressed with staff members, additional quality assurance evaluations were conducted to ensure that processes were being followed. • Equifax's Compliance Management Program involves monitoring and testing to identify and assess regulatory compliance risks and test controls and provide relevant reporting to management. • Third-line audit program. Other assurance activities include: • Systems checks and controls, including exception reporting.

		• Risk management processes. • Breach and incident reporting. • Tracking of resolution of incidents, breaches, and recommendations from assurance activities through the Corrective Actions Register and Compliance Incident Reporting Tool. • Identification of issues (systemic or one-off) through support from the Head of Legal NZ or the Compliance Team. • Compliance attestation process.
(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.	Equifax has a wide range of policies, procedures, and controls to ensure that the information that it holds is protected by reasonable security safeguards. As per last year's report, the scope of the Independent Review did not include a security audit or technical analysis. However, based on the documentation reviewed and information obtained through interviews, the security of information appears robust. • Equifax in New Zealand complies with parent company Equifax, Inc.'s Information Security Program. The Information Security Program comprises a range of policies, technical, administrative, and physical safeguards to manage risks and technical requirements. The AU/NZ regional information security team is part of the wider global information security team. • Equifax, Inc. holds Information Security Management System ISO/IEC 27001 certification. • Security incidents are monitored and addressed in real-time according to Equifax's global Technology/Security Incident Communication Procedures. • Locally, staff KPIs include a link to security awareness, leading to a good understanding of the importance of following security requirements in individuals' roles.
(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 has comprehensive processes and system controls for consumer access to credit information and the correction of credit information. Equifax provides easy-to-understand explanatory documentation to consumers about their credit report and consumer rights. As per the previous year's report, monitoring activities to ensure reasonable compliance with the Code include: • Staff processing access and correction requests receive comprehensive training. If

		training issues are identified (including through peer review, quality assurance evaluations, live call monitoring, and systems error logs), staff receive coaching to prevent recurrence. • The processing of credit reports primarily occurs overnight by automated systems, although some reports are handled manually by customer service agents. When issues arise, error logs are generated, and these cases are passed back to customer service agents for resolution. • There are systems controls to ensure that access and corrections requests are completed within timeframes. Where required, these are also monitored manually. • Monthly statistics, including correction requests (related to complaints), are reported to management for review on a monthly basis.
(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 has several measures in place to, as far as reasonably practicable, avoid the incorrect matching of information held. • Equifax has a matching algorithm in place to avoid incorrect matching as far as it is practicable. • Customer Services team staff are trained to recognise incorrect matching and arrange for corrections in line with the correction process. • Matching accuracy is reported every month to management. • Equifax is working on a project to proactively flag and separate twins' files that could potentially be mixed. The project was carried out during the reporting period, and the current solution was deployed into the production environment on 9 July 2024, affecting 82,500 master files containing data on twins of different genders. The project is currently assessing the impact following implementation and will consider the next steps, such as addressing data for twins of the same gender, once this assessment is complete.

(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.	A range of activities are in place to ensure reasonable compliance with the Code with respect to ensuring that information is accurate, up-to-date, complete, relevant, and not misleading. These include: • Data ingestion standards, processes, and controls. • Requirements for quality, accuracy, completeness, and timeliness of data provided to Equifax are included in subscriber agreements, and data is checked before it is imported. • Pre-ingestion checks are completed to identify whether a credit provider has provided an incorrect file. Where a pre-load threshold is breached, an investigation is undertaken and escalated to the account manager if relevant. • Files from suppliers/credit reporters are expected within set timeframes. When the tracking process identifies that it is not obtained on time, an escalation process is started. • Retention policies and processes, including automated purging of information in compliance with the Code. • Review of matching logic to improve the accuracy of information. • Identification of areas for improvement are made and solutions are implemented. For example, an improvement to the process where debt purchases were transferred between debt collectors was implemented during the period. • Correction processes, both credit provider and consumer initiated. Review and reporting of statistics to identify issues. • The credit default deletion processes, which include bulk deletions and single deletions, allow for the removal or amendment of defaults. The NZ Credit Default Deletions Process Audit conducted during the period suggested certain enhancements to these processes to ensure consistency across both bulk and single deletions. Changes were also made to the process where deletions were requested for reasons of fraud or the death of the consumer.

(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).*	As per last year's report, Equifax has the following in place in relation to reporting and retention of credit information: • Retention periods are integrated into systems, a process known as 'purging'. Once purged, the information cannot be retrieved, but there is a log of the deletion. • The NZ Record Retention Register outlines the applicable purge rules. • Error logs are created where failures or issues are identified. An error log would be investigated and resolved promptly. • Retention and deletion are also subject to Equifax's Global Retention Policy.
(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	There is evidence that Equifax monitored the processing of direct marketing lists appropriately. Direct marketing lists are processed only when the criteria in Schedule 10 is met, and the requirements are explicitly set out in an agreement with subscribers. The controls include Equifax undertaking the processing on behalf of the subscriber, and not returning the results directly to the subscriber.

(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.	Equifax has documented processes around the suppression of credit information and the release or cancellation of a suppression request where an individual may be a victim of fraud. These processes are consistent with Schedule 8. After the Latitude Finance data breach in 2023, Equifax made a permanent change to the suppression process. Before the breach, Equifax used to give consumers a copy of their credit file as a standard part of the process, which was over and above the requirements of the Code. However, due to the high volume of suppressions after the breach, providing a credit file added extra pressure to complete the process on time. After analysis of the process, Equifax decided to stop providing a credit record as part of the request. As noted in last year's report, Equifax has the following mechanisms in place to ensure that suppressions are processed appropriately: • Suppressions are actioned on the day that the request is made. The Customer Services team monitors requests throughout the day to ensure that they are dealt with promptly. • Suppression requests are mostly processed overnight by the Robot. Any errors are identified and corrected, as necessary. If suppressions are processed automatically, emails containing relevant information, including the PIN, are sent out. Error logs are checked to ensure all necessary emails have been sent. • Some suppressions are completed manually by the Customer Services team if there are known issues, such as a name with too many characters. • There are system controls in place to monitor extension timeframes and manual monitoring is also carried out. • Requests for release and cancellation are closely monitored. • Quality assurance assessments are conducted when processes change. For example, when the supply of credit files was removed from the suppression process, additional quality assurance assessments were carried out to ensure compliance with the new process.

(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 has processes in place to manage complaints. These processes are consistent with Clause 7. • Escalated correction requests are treated as complaints. Complaints are recorded in Service Now, and timeframes are monitored. Customer Services management receives monthly reports on complaints. Mixed file correction requests are now recorded as incidents. • Complaints that qualify as incidents are reported using the Compliance Incident Reporting Tool. The tool ensures that complaints are monitored until resolution, and incidents are reported quarterly to the RCSC. • Where required, privacy-related complaints may be escalated to the Head of Legal NZ and the Compliance Manager NZ for support and oversight. • Acknowledgement, progress and outcome emails/letters are sent within prescribed timeframes. The link to the Summary of Rights is included in the acknowledgement email/letter. The Customer Services team monitors these timeframes. A second line review of NZ Complaints is planned for the last quarter of 2024.
(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), clause 7(4) and clause 8.1 of Schedule 8.	Equifax has processes in place to ensure that its website displayed accurate information that gave effect to rules 6(7)(b), 7(5)(b), clause 7(4) and clause 8.1 of Schedule 8. The previous year's report recommended correcting two issues with Equifax's website, including where a link to an external website was broken. Equifax promptly rectified these issues. The Head of Legal, New Zealand, is responsible for updating Code-related information on the Equifax NZ website. This includes formal sign-off of any changes. The Head of Legal also reviews the website from time to time to ensure that the required information is still displayed correctly.

(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 that subscribers complied with agreements and controls. • Subscriber obligations are clearly communicated, including the requirement to cooperate with monitoring activities and findings. Equifax conducts both automated and ad hoc compliance monitoring and promptly addresses any identified non-compliance, including potential suspension of subscriber accounts. • The Controls Testing and Monitoring Team conducted two subscriber reviews during this period: o The first review aimed to determine if subscribers had obtained consent before carrying out a credit check. o The second review focused on assessing whether subscribers had accessed their own credit reports, had both Credit Provider and Debt Collector access codes on the same account (which is not allowed), and if user accounts that had not been accessed within a specified period were suspended. • Where findings were identified, appropriate actions have been agreed with relevant managers and documented in the corrective actions register. These actions are closely monitored and followed up until completion.
(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.	Intelligence and security agencies are subject to the same controls and reviews as other subscribers, including random sampling. This is outlined in the standard access agreement used for intelligence and security agencies.
(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 11 in relation to tracing individuals were met.	Equifax follows an "eTrace & Address Hygiene for the Return of Money Owed" process for requests under Schedule 11 of the Code. The requirements are addressed through a statement of work that must be agreed upon and signed by the customer before any work is carried out.

Schedule 7 Section 4 Assurances

3.4 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.	Equifax has the following processes and procedures for dealing with breaches: • Incidents are reported through the Compliance Incident Reporting Tool. Root cause analysis is undertaken, and remedial actions are taken to address deficiencies. Incidents are tracked to completion and are reported to the RCSC every quarter. • Recommendations identified through audits, compliance testing, and investigations are recorded in the corrective actions register, which tracks the progress of an identified corrective action. • There are policies and procedures that support the identification, reporting, and resolution of incidents and breaches, including a Data Breach Policy for assessing whether breaches require notification to the OPC. Six incidents relating to incorrect information on a credit file, were reported in the first nine months of the reporting year. No complaints were referred from the Office of the Privacy Commissioner during this period. The Compliance Team oversees the incidents to completion. In the case of ' long-term' issues, for example, where an identified issue requires a technological fix that may require longer-term investment, the Compliance Team regularly reviews and follows up with the Technology team for progress updates. In the 2023 report, an observation was made that some customer service team-related incidents (for example, mixed files or correction requests) that are dealt with immediately are not recorded as incidents. Since 1 May 2024, Equifax records these types of incidents in the Compliance Incident Reporting Tool. This resulted in 57 additional incidents being reported by the end of June 2024. The Compliance Team is working with the Customer Service Team to collect and act on feedback to improve the process around this new reporting requirement. While conducting walkthroughs of some

		customer service processes, two instances sampled could be categorised as needing to be reported as incidents: • During the busy period following the Latitude Finance Breach, a request for a credit report processed 2 July 2023 took 11 business days to process, which was 1 day longer than the usual reporting period. The Customer Service team experienced a significant increase in workloads during this period. Workloads for July 2023 were 307.8% higher compared to the same period in 2022. Equifax closely monitored the situation and found that processing requests outside of timeframes was rare. • In another situation, a customer service team agent made an error by sending the wrong credit report to a subscriber. The mistake was discovered and promptly corrected. However, it was not reported to the manager or team leader as per the standard procedure. The team leader committed to addressing the issue with the responsible agent, reporting the incident retrospectively and reminding the entire customer services team of the requirement to log incidents when they arise.
(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.	Two recommendations and one opportunity for improvement were identified in the 2022 – 2023 report. A summary of the recommendations and opportunity for improvement and the actions taken are outlined below. <u>Recommendation 1 - Monitoring and Testing Program</u> Due to the critical role that the Monitoring and Testing Plan takes in the overall Compliance Program and the higher-risk nature of the reviews not able to be started this year, Equifax should identify and implement strategies for increasing second-line monitoring activities to ensure that it is satisfied that it follows its policies, procedures, and controls, particularly for higher risk areas of the Code. <u>Actions taken</u> A Compliance Manager NZ was hired in April 2024. The responsibilities of the role include carrying out second-line monitoring activities for New Zealand, including monitoring activities related to the Code.

		Recommendation 2 – Website Information It was recommended that Equifax correct the two issues identified. In addition, a process should be implemented to regularly review the information on the website to ensure that it complies with the Code. A Compliance or Legal team member with knowledge of Code requirements should approve any changes to website information related to the Code. Actions taken The issues identified with the Equifax website were fully remediated on 17 August 2023. The Head of Legal NZ must sign-off only any Code related changes to the website before they are implemented. The Head of Legal NZ also conducts spot-checks to ensure that the website remains correct. Opportunity for improvement – Review of Incidents There may be some benefit to the Compliance team and resulting incident reporting to review Customer Services Team statistics to identify opportunities (if any) to enhance its reporting of incidents. Actions taken As noted above, from 1 May 2024, Equifax now records mixed file incidents in the Compliance Incident Reporting Tool. This resulted in 57 additional incidents being reported by the end of June 2024. The Compliance Team is working with the Customer Service Team to collect and act on feedback to improve the process around this new reporting requirement.