



# Equifax New Zealand Information Services and Solutions Limited

Assurance Report

Year ending 30 June 2023

# Table of Contents

<b>1. Introduction</b>	<b>3</b>
<b>2. Process of Review and Reporting</b>	<b>3</b>
Overview of the Assurance Reporting Process	3
Assurance Review Committee	5
Independent Person	6
Independent Person's Report Summary	6
<b>3. Summary of Assurances</b>	<b>8</b>
Schedule 7 Section 1 Assurances	8
Schedule 7 Section 2 Assurances	8
Schedule 7 Section 3 Assurances	13
Schedule 7 Section 4 Assurances	22

## 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 Privacy Commissioner 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 2022 to 30 June 2023 (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
<ul style="list-style-type: none"><li>• Commencement of the Annual Compliance Program and periodic Assurance Review Committee meetings</li><li>• Implementation of the Equifax Compliance Program, incorporating Code compliance as the driving force for compliance activities for the reporting year</li><li>• Completing the obligation register and confirming controls through the attestation process.</li></ul>	<ul style="list-style-type: none"><li>• Appointment of Independent reviewer</li><li>• Communication with the Assurance Review Committee</li><li>• Interviews with the Independent Reviewer Obligation Owners</li><li>• Documentation/Support review along with agreed testing</li></ul>	<ul style="list-style-type: none"><li>• Presentation of Independent Person's findings to the broader Assurance Review Committee</li><li>• Deliberation on the Independent Person's findings by the Committee</li><li>• Addressing the Committee's concerns and developing a correction action plan</li><li>• Report preparation and sign off by the Committee to be submitted</li></ul>

- 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:

<b>Step</b>	<b>Process Description</b>
Step 1: Attestations	<p>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.</p> <p>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.</p>
Step 2: Independent review	<p>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.</p> <p>This was done through document reviews, interviews, and testing.</p> <p><i>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.</i></p>
Step 3: Review of results	<p>The results of both the attestation and review process were presented to the Assurance Review Committee for discussion, along with any recommendations and improvements.</p> <p>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.</p>
Step 4: Assurance Report	<p>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.</p>

## 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<sup>1</sup>.

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

<b>Angus Luffman (Chair)</b>	Managing Director, New Zealand
<b>Alana Hampton</b>	GM – Enterprise Risk Management and Compliance, Australia and New Zealand
<b>Bob Sparshatt</b>	Chief Data Officer, Australia and New Zealand
<b>Suellen Heintz</b>	GM, Product Development & Customer Centered Design
<b>Wayne Williamson</b>	Chief Information Security Officer - Australia, New Zealand and Emerging Markets
<b>Deborah Malaghan</b>	Head of Legal, New Zealand
<b>Alexander Marwedel</b>	Head of Technology, New Zealand
<b>Paul Dunne</b>	GM - Customer Services, Australia and New Zealand
<b>Nick Foster</b>	Head of Solutions and Marketing Services
<b>Geoff Hawkins</b>	Head of Risk and Business Resilience, Australia and New Zealand
<b>Elaine Toon</b>	Senior Manager - Regulatory Compliance & Governance
<b>Michelle Olbricht</b>	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.

---

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

## **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.
- 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 one (201) documents were reviewed and assessed against the requirements of the Code.
  - Interviews with thirteen (13) key staff. The list of interviewees is included as Appendix 2.
  - 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, three areas were chosen for additional focus. This included walk-throughs, process analysis and sample testing (as appropriate) of the following topics:
- Access requests,
  - Correction requests, and
  - Complaints management.
- 2.17 The Independent Person has identified one area of the Code where Equifax has not had monitoring activities in place to ensure reasonable compliance concerning the information it displays on its website. A recommendation has been made to remediate the issues identified.
- 2.18 There are no other 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.

- 2.19 The Independent Person concluded that, in relation to the Reporting Period, and except for the issue noted above, there was sufficient evidence that Equifax complied with the obligations of the Code relating to the following:

#### **Policies, procedures, controls and subscriber agreements**

- 2.19.1 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.

#### **Monitoring of policies, procedures, controls and subscriber agreements**

- 2.19.2 Equifax's internal assurance processes are based on the three lines of defence, in line with accepted good practice.
- 2.19.3 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.
- 2.19.3 Equifax has in place a second line risk and compliance function, which includes a monitoring and testing function. Due to a vacant role, there was a reduced number of reviews completed during the period which resulted in higher risk aspects of the Code not being reviewed, such as complaints and corrections. This does not represent non-compliance with the code, as other existing assurance activities, such as management oversight and quality checking, support EFX's continued compliance with the Code. A recommendation has been made 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.
- 2.19.4 A second recommendation has been made concerning the information required to be displayed on the Equifax website. In the case of translated versions of the Summary of Rights, the links provided to the Office of the Privacy Commissioner website were broken. Regarding information on suppressions, the Independent Person could not find the complete list of required information through links or keyword searches (although a webpage does exist with this information, found only through reviewing an internal process). It was recommended that Equifax correct the two issues identified, which is now underway. In addition, it was recommended a process should be implemented to regularly review the information on the website to ensure that it complies with the Code; and a Compliance or Legal team member with knowledge of Code requirements should approve any changes to website information related to the Code. This latter recommendation is current policy.

#### **Actions taken on deficiencies identified**

- 2.19.5 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.
- 2.19.6 Of the recommendation and opportunity for improvement identified in the last report, Equifax has considered these and believe that it is in compliance with the Code. Nevertheless, it has indicated that it will consider these when planning for 2023-2024. It is acknowledged that Equifax is constrained in second-line monitoring and has not been able to complete its planned Monitoring and Testing Program.

2.19.7 An opportunity for improvement has been identified concerning incident reporting. During the review, it was identified that there are several complaints and mixed file issues that occur monthly via the Customer Services Team. These complaints and mixed file issues are proactively managed and closed, and statistics are reported to management monthly. It may be possible that some of these complaints, twin and non-twin mixed files could, although not verified by the Independent Person, meet the definition of a compliance incident and should be reported through the Compliance Incident Reporting Tool. 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.

### 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.

3.2 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

3.3 Assurances relating to policies, procedures, controls and subscriber agreements

Section 2	Expectation per the Code	Findings of the Independent Person and Equifax
-----------	--------------------------	--



(a)	<p>In relation to the applicable period, Equifax had policies in place that give effect to the requirements of the Code.</p>	<p>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.</p> <p>Ownership of policies is well understood and is documented in the Obligations Register. Obligation owners regularly attest to compliance currency of processes or controls or confirm changes to processes or controls.</p> <p>A new policy, the Policy on Standards and Requirements for Australia and New Zealand, forms part of the Compliance Management Program. It prescribes a set of consistent standards and requirements for developing, issuing, and maintaining Regional Corporate Policies. Oversight of Equifax's policy framework is delegated to the Risk, Compliance and Security Committee's Policy Sub-Committee, which meets at least four times per year.</p>
(b)	<p>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.</p>	<p>Equifax had policies in place to ensure that any arrangements with related companies accord with clause 4(2) of the Code.</p> <p>There are five New Zealand entities, four of which are holding companies. Equifax New Zealand Information Services and Solutions Limited is the operating entity.</p> <p>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.</p> <p>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.</p>

(c)	<p>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.</p>	<p>Equifax has internal procedures and controls in place to give effect to the policies and requirements of the Code.</p> <p>Internal procedures and controls include:</p> <ul style="list-style-type: none"> <li>• An overarching compliance management program to oversee compliance with obligations and requirements.</li> <li>• Ownership of obligations and controls are assigned, and an attestation process is undertaken by the Compliance function quarterly.</li> <li>• A range of process and procedure documentation for functions across Equifax. It was noted that most of the Customer Service team process documents were updated within the period to reflect the IT system's menu changes.</li> <li>• Organisation-wide training at onboarding and key training is repeated annually. There is also team-specific training at onboarding and at regular intervals. Additional training or education is provided to Equifax employees and subscribers (where applicable) when issues are identified.</li> <li>• First-line quality assurance reviews, peer reviews and manager oversight. Second-line monitoring and testing program. Third-line audit program.</li> <li>• System controls and checks. For example, system controls are embedded into the data ingestion process. Systems controls embedded into the Customer Service RPA (robot) processes. Error messages are produced, investigated, and resolved.</li> <li>• A wide range of global security controls.</li> <li>• Incident management procedure and system to record incidents and breaches. Oversight of corrective actions.</li> <li>• Privacy Impact Assessments are required for all changes.</li> </ul>
-----	---	--

(d)	<p>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.</p>	<p>Equifax has comprehensive procedures in place for responding to access requests as required by Rule 6.</p> <p>Written procedures are comprehensive. The Customer Services team members are provided comprehensive on-the-job training and ongoing support.</p> <p>Procedures and controls include:</p> <ul style="list-style-type: none"> <li>• Verification of identity and contact details.</li> <li>• Third-party waiver process.</li> <li>• Automated processes via RPA (robot), which verifies requirements and sends automated credit reports. Error messages are investigated and resolved.</li> <li>• Credit reports are encrypted, and a separate email is sent to the requestor with a password.</li> </ul> <p>Procedures to avoid bundling of authorisations that may circumvent the Code's prohibitions on marketing and direct marketing include:</p> <ul style="list-style-type: none"> <li>• Use of privacy impact assessments for all new use requests.</li> <li>• Separation of the Marketing database from the Bureau, with restrictions on access.</li> <li>• Terms and conditions in subscriber agreements that explicitly prohibit use for marketing.</li> <li>• Internal review of multiple requests.</li> <li>• System rejection of bundled requests.</li> </ul>
-----	---	--

(e)	In relation to the applicable period, Equifax provided information and training to its staff to ensure compliance with the policies, procedures and controls.	<p>Equifax provided information and training to its staff to ensure compliance with the policies, procedures and controls.</p> <p>Information and training provided to Equifax staff includes:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Training records are maintained, and non-completion is escalated.</li> <li>• 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 November 2022.</li> <li>• Other online training is also refreshed regularly.</li> <li>• 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.</li> <li>• Other resources include the Privacy Toolkit intranet page and regular broadcasts/emails to staff. Equifax participated in Privacy Week in May 2023.</li> </ul>
(f)	In relation to the applicable period, Equifax ensured that subscriber agreements that complied with Schedule 3 were in place before disclosing credit information.	<p>There is evidence that subscriber agreements that complied with Schedule 3 were in place before disclosing credit information.</p> <p>Equifax's subscriber onboarding policy, process and systems do not allow subscribers access to credit information without meeting set criteria.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• The Equifax NZ Subscription Process Document provides detailed steps for onboarding, including key approval guidelines.</li> <li>• The Onboarding Leader reviews and approves/declines all new subscribers based on set criteria.</li> </ul>

		<ul style="list-style-type: none"> <li>System controls are in place to ensure that this requirement is met.</li> </ul> <p>It is understood that Equifax does not include testing of compliance with this aspect of the Code, as per previous year's reports. Per Equifax's comments concerning last year's opportunity to widen the scope of subscriber audits, it will continue to consider monitoring and testing additional aspects of the Code.</p>
(g)	In relation to the applicable period, Equifax ensured that access arrangements under Schedule 4 were in place before disclosing credit information.	<p>There is evidence that Equifax ensured that access arrangements under Schedule 4 were in place before disclosing credit information.</p> <p>As noted with the findings under f. (above), Equifax's subscriber onboarding policy, process and systems do not allow access to credit information without meeting set criteria. It is understood that the intelligence community must meet the same criteria as other subscribers, including requiring consent for an individual applying to join the intelligence and security agency (the difference being that the footprint of the agency is not shown).</p>

### Schedule 7 Section 3 Assurances

#### 3.4 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.	<p>There is reasonable assurance that Equifax undertook monitoring activities to ensure reasonable compliance with the Code, including that it followed its own policies, procedures and controls.</p> <p>Equifax has several ways of undertaking monitoring activities to ensure that it complies with its own policies, procedures and controls. These include:</p> <ul style="list-style-type: none"> <li>First-line quality assurance reviews, peer reviews and manager oversight.</li> <li>Second-line monitoring and testing program. Compliance Monitoring and Testing Standards govern this.</li> <li>Third-line audit program.</li> </ul> <p>Other assurance activities include:</p> <ul style="list-style-type: none"> <li>Systems checks and controls, including exception reporting.</li> <li>Risk management processes.</li> <li>Breach and incident reporting.</li> </ul>

		<ul style="list-style-type: none"> <li>• Tracking of resolution of incidents, breaches and recommendations from assurance activities through the Corrective Actions Register and Compliance Incident Reporting Tool.</li> <li>• Identification of issues (systemic or one-off) through support from the Head of Legal NZ or the Compliance Team.</li> <li>• Compliance attestation process.</li> </ul> <p>Monitoring and testing is a key component of Equifax's Compliance Management Program. It helps Equifax identify, assess and monitor regulatory compliance risks, test controls and provide reporting to management as applicable. Monitoring and testing compliance with the Code is included in the CTM NZ Review Plan annually. It is understood that the plan is developed based on an internal assessment of risk, which is appropriate for a second-line monitoring and testing program.</p> <p>The CTM NZ Review Plan included three second-line monitoring and testing reviews for the year. However, only one scheduled second-line monitoring and testing activity was completed for the applicable year. The fieldwork for the Subscriber Review is complete, and the draft report is with managers for feedback. However, the Complaints and Corrections reviews could not be started due to resourcing constraints. Specifically, the Compliance Officer New Zealand left the organisation in November 2022. This role was responsible for completing fieldwork for reviews conducted in New Zealand. It is understood that this role had not been replaced as at the end of the reporting period due to a hiring moratorium. Alternative resourcing from the Internal Audit team was sought and agreed to, but the reviews could not be started due to that team's own resourcing constraints.</p>
(b)	<p>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.</p>	<p>Equifax has a wide range of policies, procedures and controls to ensure that the information that it holds is protected by reasonable security safeguards.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• 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</li> </ul>

		<p>safeguards to manage risks and technical requirements. The AU/NZ regional information security team is part of the wider global information security team.</p> <ul style="list-style-type: none"> <li>• Equifax, Inc. holds Information Security Management System ISO/IEC 27001:2013 certification, most recently issued in February 2023. The scope of the certificate includes satellite offices, including Equifax's Auckland office.</li> <li>• Security incidents are detected and managed in real-time in line with the Equifax global Technology/Security Incident Communication Procedures.</li> <li>• Locally, staff KPIs include a link to security awareness, leading to a good understanding of the importance of following security requirements in individuals' roles.</li> </ul>
(c)	<p>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.</p>	<p>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.</p> <p>Monitoring activities to ensure reasonable compliance with the Code included:</p> <ul style="list-style-type: none"> <li>• Staff processing access and corrections requests are given comprehensive training. If training issues are identified (including via peer review, monitoring, systems error logs, and live call monitoring), staff are provided coaching to prevent recurrence.</li> <li>• Credit reports are processed overnight by an automated process, and if applicable, error logs are reviewed, and issues are corrected.</li> <li>• There are systems controls to ensure that access and corrections requests are completed within timeframes. Where required, these are also monitored manually.</li> <li>• Monthly reporting of statistics, including corrections requests (closely linked with complaints), is provided to management for review.</li> <li>• There are processes in place to make corrections requested by credit providers. These can be actioned per request, or where bulk corrections are required, these are handled by the Data Ingestion team.</li> </ul> <p>As noted under a. (above), planned second-line monitoring and testing of corrections did not occur</p>

		due to resourcing constraints.
(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.	<p>Equifax has several measures in place to, as far as reasonably practicable, avoid the incorrect matching of information held.</p> <ul style="list-style-type: none"> <li>• Equifax has a matching algorithm in place to avoid incorrect matching as far as it is practicable.</li> <li>• Customer Services team staff are trained to recognise incorrect matching and arrange for corrections in line with the correction process.</li> <li>• Matching accuracy is reported every month to management.</li> </ul> <p>Where incidents occur, root cause analysis is undertaken. Specifically, in February 2023, a mixed file that disclosed elements of a twin's information resulted in a complaint reported to the Office of the Privacy Commissioner. This incident prompted the need for an interim solution until the bureau transformation to an updated system occurs. The approximate dates for the implementation of the solution are yet been confirmed.</p>



(e)	<p>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.</p>	<p>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:</p> <ul style="list-style-type: none"> <li>• Data ingestion standards, processes and controls.</li> <li>• 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.</li> <li>• 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. This process was implemented following an incident where an error by a client accidentally 'closed' a number of accounts that were still open.</li> <li>• 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.</li> <li>• Retention policies and processes, including automated purging of information in compliance with the Code.</li> <li>• Review of matching logic to improve the accuracy of information.</li> <li>• Correction processes, both credit provider and consumer-initiated. Review and reporting of statistics to identify issues.</li> </ul>
-----	--	--

(f)	<p>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 (<i>Retention of credit information</i>) and Schedule 1 (<i>Maximum reporting periods</i>).</p>	<p>Equifax has the following in place in relation to reporting and retention of credit information:</p> <ul style="list-style-type: none"> <li>• Retention periods are embedded into systems; this process is known as 'purging'. The information cannot be retrieved once purged. However, there is a log of the deletion. For example, once a default has reached its maximum period of 5 years, it is automatically purged from the system.</li> <li>• A default can be corrected by removing or amending it manually. The Customer Services team has documented processes to complete this.</li> <li>• There is a Bulk Consumer Default Deletions process where multiple defaults can be removed if incorrect.</li> <li>• The NZ Record Retention Register outlines the applicable purge rules.</li> <li>• Error logs are created where failures or issues are identified. The error log would be investigated, and issues resolved, although it was indicated during interviews that this was rare.</li> </ul> <p>Retention and deletion are also subject to Equifax's Global Retention Policy. An annual attestation process is included as part of the policy, as well as random audits of compliance with the Policy from a global perspective.</p>
(g)	<p>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</p>	<p>There is evidence that Equifax monitored the processing of direct marketing lists appropriately.</p> <p>It is understood that 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.</p>

(h)	<p>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.</p>	<p>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.</p> <p>It is noted that the process for Suppressions was widened and made more accessible for consumers where the recent Latitude Financial Services breach had impacted them.</p> <ul style="list-style-type: none"> <li>• Suppressions are completed on the day that the request is made. The Customer Services team monitors requests throughout the day to ensure these timeframes are met.</li> <li>• Suppressions are generally processed overnight by an automated process, and if applicable, error logs are reviewed, and issues are corrected.</li> <li>• Where suppressions are processed automatically, emails are sent with relevant information, including the PIN. Again, error logs will identify if emails with information have not been sent.</li> <li>• Some suppressions are completed manually by Customer Services team staff if there are known issues, such as a name with too many characters.</li> <li>• System controls are in place to monitor extension timeframes. Manual monitoring is also undertaken.</li> </ul> <p>Release and cancellation requests are monitored.</p>
-----	---	--

(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.	<p>Equifax has processes in place to manage complaints. These processes are consistent with Clause 7.</p> <ul style="list-style-type: none"> <li>• Escalated corrections requests are considered complaints. The receipt of the complaint is recorded in the 'Service Now' processing system, and timeframes are monitored. Complaints are reported every month to Customer Services management.</li> <li>• Complaints considered incidents (for example, the twin matching incident from February 2023) are reported to the Compliance Incident Reporting Tool. Once reported through the tool, complaints are monitored through to resolution. Incidents are reported quarterly to the RCSC.</li> <li>• Where required, complaints may be escalated to the Head of Legal, NZ, for oversight.</li> <li>• 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.</li> </ul> <p>As noted under a. (above), planned second-line monitoring and testing of complaints did not occur due to resourcing constraints.</p>
(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.	<p>When reviewing Equifax's website, two issues were identified by the Independent Person.</p> <ol style="list-style-type: none"> <li>1 The Equifax website contained links to translated versions of the Summary of Rights as required by clause 7(4).<sup>2</sup> However, each of these links were directed to the Office of the Privacy Commissioner website, and due to updates on that website, each link was broken. As a result, no translations of the Summary of Rights were available. This issue has now been rectified with links to the PDF translations.</li> <li>2 The full information required to be made available on Equifax's website under clause 8.1 of Schedule 8<sup>3</sup> related to suppressions</li> </ol>

<sup>2</sup> A credit reporter must conspicuously display on the credit reporter's website— (a) a copy of the Summary of Rights; and (b) any official translation of the Summary of Rights released by the Privacy Commissioner

<sup>3</sup> Credit reporter to make available details of request processes 8.1 A credit reporter must make available on request and on the credit reporter's website details of the credit reporter's processes to make an initial request, extension request, release request and cancellation request which should include, amongst other matters, guidance on— (a) the supporting documentation that might typically be expected; and (b) the requirements for agents making applications on behalf of individuals; and (c) the credit reporter's criteria for deciding on an extension request; and (d) the likely processing time for requests; and (e) any arrangement between credit reporters of the type anticipated in clause

		<p>could not be found in its entirety.</p> <p>Some, but not all, of this information can be found in the FAQs.</p> <p>When reviewing the Suppression Processing Document V1.2, a link to the missing content was identified. This information cannot be found via links or keyword searches. Rectification of this issue is underway.</p>
(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.	<p>Equifax undertook appropriate monitoring activities to ensure reasonable compliance with the Code, including that subscribers complied with agreements and controls.</p> <ul style="list-style-type: none"> <li>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).</li> <li>The Monitoring and Testing team has completed the annual Subscriber Monitoring and Testing Review. At the time of the independent review, the report was in draft with management comments on recommendations being collated. The scope of the review was to ensure that subscribers obtain consent from individuals before performing credit checks. It is noted that compliance with other aspects<sup>4</sup> of the agreements was not reviewed.</li> </ul>
(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.	<p>The agreement with the SIS is subject to review per the scheduled subscriber audits undertaken by the Monitoring and Testing team.</p> <p>Intelligence and security agencies are subject to the same controls and reviews as other subscribers.</p>

---

1.4 for sharing and acting upon initial requests.

<sup>4</sup> Assurances relating to policies, procedures, controls and subscriber agreements (f), (g)

Assurances relating to monitoring of policies, procedures, controls and subscriber agreements (k), (l), (m)

(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 for the return of money were met.	<p>The requirements are actioned through a standard contract for tracing for the return of money.</p> <p>Tracing for the return of money is a process undertaken by Equifax on behalf of subscribers, including undertaking communications on the subscriber's behalf. As such Equifax has complete control of this process.</p>
-----	---	--

### Schedule 7 Section 4 Assurances

#### 3.5 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.	<p>There is reasonable assurance 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, the credit reporter investigated that breach and, where appropriate, took prompt remedial action. No recommendations have been made. However, an opportunity for improvement has been identified.</p> <p>Evidence has been provided that, 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.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Recommendations identified through audits, reviews, investigations, complaints, or incidents are recorded in the corrective actions register.</li> <li>• A corrective actions register is used to track breaches, incidents and progress made on recommendations made because of audit, review or investigation.</li> <li>• There are policies and procedures which support the identification, reporting and resolution of incidents and breaches.</li> </ul>

		<p>Of the seven incidents reported to the RCSC, all incidents were promptly investigated and resolved (as far as practicable).</p> <p>It was noted by the Independent Person that seven incidents seemed to be a low number, given the nature of Equifax's business. However, the Independent Person has not determined that this number represents under-reporting. During the review, it was identified that there are several complaints and mixed file issues that occur monthly via the Customer Services Team. For example, in June 2023, the Customer Services Team corrected 22 twin and non-twin mixed file issues. These complaints and mixed file issues are proactively managed and closed, and statistics are reported to management monthly. It may be possible that some of these complaints, twin and non-twin mixed files could, although this was not verified by the Independent Person, meet the definition of a compliance incident and should be reported through the Compliance Incident Reporting Tool.</p> <p>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.</p>
(b)	<p>In relation to the applicable period, where a deficiency was identified in the previous year's report, Equifax, where appropriate, took prompt remedial action.</p>	<p>One recommendation and one opportunity for improvement were identified in the 2021 – 2022 report. A summary of the recommendation and opportunity for improvement, as well as Equifax's responses, are outlined below.</p> <p><u>Recommendation</u> The planned monitoring of compliance with the requirements to not store personal and credit information in GSuite should be prioritised and undertaken from this year.</p> <p><u>Equifax response</u> EFX considered this recommendation, and after review, determined that it is in compliance with the Code requirements. However, we consider this to be an opportunity for improvement and, as a result, this monitoring effort is continuing to be prioritised and fine-tuned, with the work on this initiative continuing into 2024.</p> <p><u>Opportunity for further improvement</u> The scope of subscriber audits undertaken by Equifax should be widened, to focus on all relevant areas of compliance with the agreements and the</p>

		<p>Code.</p> <p><u>Equifax response</u></p> <p>Compliance Testing and Monitoring considered this opportunity for further improvement, and after review, determined that the subscriber audits as they were, are in compliance with the Code requirements. Despite this, CTM will consider widening the scope of these audits in due course as it prepares its future testing plans.</p>
--	--	---