COMPLIANCE POLICY

1. Purpose of this Compliance Plan

This Compliance Plan sets out the key measures the business applies in operating to ensure compliance with our obligations as a credit licensee including compliance with the National Consumer Credit Protection Act 2009.The business recognizes that the Compliance Plan is a vital instrument to achieve the best operational and compliance practices. As such, the strategic objectives of the compliance plan are to:

- promote a culture of compliance.
- identify and document key compliance obligations.
- assign responsibility for key compliance tasks.
- monitor the extent to which these obligations are being effectively carried out.
- maintain records of compliance activities.
- record our compliance performance (including breaches).
- analyse compliance data to identify systemic and recurring problems.
- continuously improve our systems and procedures.
- communicate with key stakeholders, including regulators.

2. Compliance Framework

2.1 Compliance Framework Elements

The business has adopted a formal compliance framework which is comprised of various elements, structures, policies, procedures, and systems that are collectively designed to ensure compliance with our broader compliance requirements.

The Framework consists of four main elements:

1. Structural: covers the hierarchy of persons and entities involved in the business.
2. Procedural: covers policies, procedures and systems maintained by us and our service providers.
3. Operational: covers identification and implementation of compliance requirements, reporting and rectification of issues and breaches; and
4. Maintenance: covers ongoing education and training and Monitoring of Compliance Procedures.

The structural element of the framework is the hierarchy of persons involved in the running of the business. While every person involved within the business does have compliance responsibilities, there is a clear hierarchy of responsibility. The Structural Elements include:

1. The Board of Directors;

2. Compliance Manager (Responsible Manager);
3. Credit Representatives
4. External Service Providers

The Procedural Elements of the Framework are included in various documents, including:

1. This Compliance Plan
2. Hardship Policy
3. Disputes Policy
4. Risk Management Plan
5. Responsible Lending Policy
6. Other policies, procedures and systems maintained by the business and its service providers.

The Maintenance Elements of the Framework are comprised of monitoring, reviewing and reporting functions undertaken by various parties, including the Compliance Manager, the Plan auditor, credit representatives and other service providers. The intention for the Maintenance Elements of the Framework is to ensure that the business is operated in accordance with the agreed standards, and that those standards are adequate to ensure ongoing compliance with ASIC policy and other regulatory requirements.

2.2 The Board of Directors

The Board of Directors is responsible for:

- Demonstrating a strong culture of compliance, putting compliant behaviour at the fore of all decision making.
- integrating compliance obligations into business strategies and plans.
- Ensuring compliance capabilities and performance are factored into contracts with external suppliers.
- Signing off on the reviews of the compliance programme.
- Maintaining a compliance reporting and documenting system.
- Maintaining systems for sourcing information such as complaints, feedback and other mechanisms; Monitoring overall compliance performance.
- Analysing performance to identify the need for corrective action.
- Performing their duties in an ethical, lawful and safe manner.

2.3 Compliance Manager

The Compliance Manager of the business is also the Responsible Manager. The Responsible Manager will carry out duties with regards to:

- communicating the compliance initiatives and measures to the relevant stakeholders.
- communicating compliance plans and processes to staff.
- ensuring staff education and awareness of the measures (testing the measures).

- implementing clear reporting lines for the staff and managers.
- receiving reports on those measures.
- maintaining a non-compliance register and reporting back to the business.

This document names the following person as the Compliance Manager.

1) Andrew Bell

2.4 Outsourcing Service Providers

The business may engage outsourcing of external service providers from time to time to perform specific functions in relation to the operations of the business. Notwithstanding the appointment of any external service provider, the business remains responsible for the operation of the business.

2.5 Reporting

Reports from various parties associated with the Plan form a large part of the information received by the board to help it assess the business's compliance with the Plan. Specific Reports to be tabled at the relevant meetings may include:

- Compliance Manager's Report;
- Breach Report; and
- External Service Provider Reports.

2.6 Reviewing and Amending the Plan

The Compliance Manager must review the compliance plan annually. They must also provide reports after the review regarding the continued adequacy of the Plan.

The Compliance Manager is responsible for submitting amended Plans to ASIC, and for ensuring that the Responsible Persons receive notification of the changes and access to a copy of the updated Plan.

Each time the compliance plan is updated it will be given a revised version number and the older version will be archived for a period of 7 years by saving it in the folder created on our computer server in the Compliance Folder.

3. Obligations

3.1 Compliance Conduct Standards

The business will always strive to meet our general conduct standards when delivering our financial services. As per ASIC Regulatory Guide (RG) 104, we are required to do all things necessary to ensure our financial services are provided:

1. efficiently,
2. honestly, and
3. fairly.

3.2 Compliance with Conditions of License

The business will always comply with the conditions of any government licenses, such as an Australian Credit License. This includes the following conditions of an Australian Credit Licence:

3.2.1 Key Person Requirements

If any of the key persons listed on the credit licence cease to perform their duties on behalf of the licensee with respect to its credit business, the business will within 5 business days:

- Notify ASIC in writing that the person has ceased performing their duties and the date this occurred.
- Lodge with ASIC an application for variation of this condition, including the new key person's name, address, date of commencement, duties, educational qualifications and experience.

3.2.2 Notification to Current or Former Representative's Clients

If ASIC makes a banning order against or the court makes an Order disqualifying a person who is a current or former representative of the licensee, the business will, if instructed by ASIC, take all reasonable steps to provide the following information in writing to any person in relation to whom the representative engaged in a credit activity on behalf of the licensee within a period of three years before the order was made:

- the name of the representative;
- if the representative is a credit representative, the credit representative number allocated to the representative by ASIC;
- the terms of the Order; and
- contact details of the licensee for dealing with enquiries and complaints regarding the banning or disqualification or the conduct of the representative.

3.2.3 Continuing Professional Development Requirements for Responsible Managers

The business will ensure that:

- each Responsible Manager of the business undertakes at least 20 hours of continuing professional development in each calendar year in which they perform the role of Responsible Manager for the licensee.
- the continuing professional development activities that are undertaken by each Responsible Manager are relevant to the role of the Responsible Manager with the licensee and include activities dealing with product and industry developments related to credit and compliance training on regulatory requirements applying to credit activities.
- a record of the continuing professional development activities undertaken by each Responsible Manager is maintained for each calendar year in which they perform the role of Responsible Manager for the licensee.

For more detail on this, please see this Section 8 People management section.

3.2.4 External Dispute Resolution Requirements

If the business ceases, or becomes aware that it will cease, to be a member of an approved External Dispute Resolution (EDR) scheme, the business will, within three business days of the date the licensee's membership ceased or the licensee became aware that its membership would cease:

- notify ASIC in writing of the reasons the licensee's membership of the EDR scheme ceased or will cease
- if the licensee has not obtained membership of another approved EDR scheme, give ASIC a written explanation that includes: reasons why the business has not obtained membership of another approved EDR scheme, details of the EDR scheme the licensee proposes to become a member of, details of steps that the licensee has taken, and will take, to become a member of that EDR scheme and the expected timeframe for becoming a member of that EDR scheme.

For more details the business External Dispute Resolution requirements, see Dispute Resolution policy.

3.2.5 Record Keeping Requirements

The business will keep a record of all material that forms the basis of an assessment of whether a credit contract or consumer lease will be not unsuitable for a consumer in a form that will enable the business to give the consumer a written copy of the assessment if a request is made within the prescribed period.

If the business is a credit provider for a particular credit contract but is not the original credit provider it will obtain a written copy of the assessment of whether the credit contract or consumer lease will be not unsuitable for the consumer from the original credit provider or a person (a previous assignee) to whom the rights of the original credit provider or lessor have previously been assigned or passed by law, and keep a written electronic copy of the assessment.

3.2.6 Compensation Arrangements

The business maintains a compensation arrangements policy to ensure it meets its compensation requirements.

3.2.7 Any other Requirements

The business will ensure that any other conditions that arise on an Australian credit licence will be followed.

3.3 Compliance with the Credit legislation

The business will always strive to comply with the National Consumer Credit Protection Act and the National Consumer Credit Protection Regulations. It is the responsibility of the Responsible Manager to ensure compliance with this legislation. Compliance with this legislation is maintained by the business's various compliance related policies and procedures, which must be kept up to date and on hand for all staff. The business also acknowledges that this legislation is prone to change and makes it the responsibility of the Responsible Manager to once per month check for updated versions of this legislation.

3.4 Compliance with other Legislation

The business has multiple laws that we must be aware of and abide by, such as:

- The Corporations Act 2001
- The Privacy Act 1988
- Competition and Consumer Act 2010
- Anti-Money Laundering and Counter-Terrorism Financing Act 2006

3.5 Compliance Breach Register

We maintain a Breach Register in which we record any material breaches of compliance procedures. The Responsible Manager will review the Breach Register formally each year as part of the compliance plan review and include this in our annual ASIC return. Repeat offenders will be issued warnings, and if the behaviour does not improve, may be removed as Representatives. The Breach Register is a spreadsheet and is stored on the server.

5. Risks of Noncompliance

A key part of the development of a Compliance Plan and compliance procedures is to be aware of the risks involved in noncompliance. The risks of noncompliance include, but are not limited to, the following:

- Customer complaints.
- Loss of customers.
- loss to unitholders and potential unitholder action.
- loss of business Property.
- imposition of penalty payments.
- legal sanctions.
- winding up of the business.

Complying with the business's obligations means doing the right thing and most importantly allows the business to focus on its core activities without distraction. Compliance leads to increased productivity, increased profitability and ultimately increased business value. An effective compliance programme helps to understand obligations and reduce the risk of breaching them.

6. Resources

6.1 Human Resources

The business is required to have adequate human resources to engage in our credit activities. This includes having adequate human resources for all related functions, such as hardship requests, dispute resolution, auditing, etc. We prepare and review our human resources monthly at a management level to ensure the business has up-to-date access to human resources.

In completing these reviews, several factors are considered, such as current human resources adequacy and forecasted workloads. When forecasting future workloads, consideration is given to business growth, seasonal market changes and market and legislative changes.

6.2 Financial Resources

The business is required to have adequate financial resources to engage in our desired credit activities. We prepare and review our financial position monthly at a board level to ensure the business has access to adequate financial resources. The primary source of funds for the business's loans is from the shareholders of the company and private investors.

6.3 Technological Resources

The business is required to have adequate technological resources to engage in our desired credit activities. For all our technological needs, we make use of the MIMO system.

6.3.1 Company Background

The system has been built up to provide a complete solution for businesses operating in the credit industry. The system is used to manage our business which includes tasks such as workflows for loans being processed, managing loan applications, business KPI reporting, payments (both in and out), loan tracking and exception reporting. It maintains and keeps track of incoming loan applications, existing clients, compliance procedures and credit representatives. It also includes built in email, phone, and storage services.

6.3.2 Service Monitoring

Mimo has an automated monitoring system with a dashboard and email alerts sent for critical issues. Core systems are monitored constantly with alerts triggered when thresholds are reached. This information is also reviewed regularly to assess trends and used for capacity planning.

6.3.3 Availability

Mimo is always available except during scheduled maintenance outages. Mimo is hosted at a managed off-site data-centre in Sydney by a reputable company, with UPS and backup power generator facilities. The application is load balanced across multiple web servers and application servers to provide a high level of availability and can tolerate the failure of a server with minimal interruption.

6.3.4 Backup and Recovery

Included with Mimo’s hosting at the off-site data centre are full backup and recovery services. The production servers and data are backed up constantly daily to alternative servers at different sites. The daily backups are stored for a week. A weekly archive is taken and stored for a month.

6.3.5 Disaster Recovery

There is a documented Disaster Recovery Plan, which is tested at a minimum once a year, with the results appraised by external auditors. The DR plan is revised and retested with each major infrastructure change. In the event of a disaster the systems will be recovered within 24 hours, with no more than 24 hours data loss. The disaster recovery (DR) site is at the business’s head office.

6.3.6 Security

Mimo uses multiple layers of security, including firewalls and intrusion prevention systems at the perimeter. There is also a reverse proxy server to hide the web servers and the production version of the software is only available at whitelisted

IP's. The Mimo web client uses 256bit SSL encryption for the transmission of data. All customer documents, such as bank statements and Centrelink income statements, are individually password protected by the system, so if the database is breached, the documents cannot be accessed. Mimo uses a hierarchical access control model. There are no limits to the number of levels in the hierarchy and those higher up in the hierarchy can see the data of those below them. Furthermore, access to data is restricted by the users position and access to the views in Mimo is restricted by their responsibility level. User passwords require 8 alphanumeric characters, capital and lower-case letters and a symbol. Mimo client currently uses database authentication and stores the passwords in encrypted form with a DES encryption algorithm. Virus scanners and spam filters are also employed internally at the business to prevent intrusion. The business will also employ external security consultants to perform a vulnerability assessment and conduct an ethical hacking exercise on an annual basis.

6.3.7 Development & management

While the software is developed by Squaresoft Media, and is leased out to use, further system enhancements can be requested. Depending on the development required, Squaresoft does offer to complete these developments at little to no cost if it will improve the software for their other customers.