Respecting your Privacy and the Australian Privacy Principals effective September 2018

Who are we?

We', 'us' and 'our' refer to FC Capital Holdings Pty Limited ACN 605 121 364 and our related businesses ("**FC Capital**" or "**FCC**"). Our related businesses include FC Capital Holdings Pty Ltd, FC Operations Pty Ltd, First Class Funds Management Pty Ltd, First Class Securities Pty Ltd, FC Capital Pty Ltd and Transact Payments Pty Ltd.

Our commitment to protect your privacy

The privacy of your personal information is important to us at FCC. We are committed to respecting your right to privacy and to protecting your personal information.

We recognise that any personal information we collect about you will only be used for the purposes we have collected it for or as allowed under the law. It is important to us that you are confident that any personal information we hold about you will be treated in a way which ensures protection of your personal information.

We are bound by the Australian Privacy Principles "APP", the Privacy Act 1988 and Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Commonwealth) and any other applicable laws and codes with respect to credit reporting and collection, storage, use and disclosure of personal and financial information.

About this Privacy Policy

This Privacy Policy outlines how we manage your personal information. Further, it describes the nature of the personal information held, the purposes for which it is held and the manner in which it is collected and disclosed.

Our Privacy Policy applies to all your dealings with us whether through one of our franchisees, other FCC organisations or via our websites. However, depending on the FCC organisation with which you deal, further privacy information may apply in addition to the matters discussed in this document. For example, please see *Our Websites* noted below.

We encourage you to check our websites regularly for any updates to our Privacy Policy.

Personal information we collect and hold

"Personal Information" is information which may be used to identify an individual, including name, age, date of birth, gender, occupation, contact details (e.g. address, phone number, email address), residency status, country of birth, nationality, tax residency, tax file number, information contained in identity documents (e.g. passport number, driver licence number), financial information, information about your use of our products and services, credit related information or other information FCC considers necessary.

When you use our website or mobile applications we may collect information about your location or activity including IP address, telephone number and whether you have accessed third party sites, the date and time of visits, the pages that are viewed, information about the device used and other user location information. We collect some of this information using cookies (for more information please see the Website Terms of Use/Policy at http://www.finstro.com.au/webprivacypolicy

Credit-related information means:

- ***Credit information***, which is information which includes your identity; the type, terms and maximum amount of credit provided to you, including when that credit was provided and when it was repaid; *repayment history information*, *default information* (including overdue

payments); payment information; Commercial and Consumer credit information from a Credit Reporting Body; Customer Identification by a Credit Reporting Body; financial information; new arrangement information; details of any serious credit infringements; court proceedings information; personal insolvency information and publicly available information; and

- ***Credit eligibility information***, which is credit reporting information supplied to us by a credit reporting body, and any information that we derive from it.

We use your credit-related information to assess your eligibility to be provided with finance. Usually, credit-related information is exchanged between credit and finance providers and credit reporting bodies.

By law, we are required to collect and store this information in accordance with prudent risk management, banking and anti-money laundering and counter terrorism financing legislation.

Why we collect your personal information

We collect personal information for the purposes of assessing your application for finance and managing that finance, establishing your identity, contacting you, managing our risk and to comply with our legal obligations.

Collecting your personal information

If you are acquiring or have acquired a product or service from an FCC organisation, we will collect and hold your personal information for the purposes of:

- providing you with the relevant product or service (including assessing your application and identifying you)
- managing and administering the product or service protecting against fraud.

FCC organisations may also collect your personal information for the purpose of informing you of FCC products and services that may better serve your financial, business and lifestyle needs, or to notify you of promotions or other opportunities in which you may be interested.

We will, if it is reasonable or practicable to do so, collect your personal information from you. This may happen when you fill out a product or service application or an administrative form (e.g. a change of address form), or when you give us personal information over the telephone, or through an FCC organisation's website.

In certain cases we may collect your personal information from third parties. For example, we may need to collect personal information from a credit reporting body, your representative (such as a legal adviser), your financial adviser, any publicly available sources of information, or from any of the other organisations identified below under "Using and Disclosing Your Personal Information". The personal information is securely stored by a 3rd party storage provider.

We will not ask you to supply personal information publicly over Facebook, Twitter, or any other social media platform that we use.

Using and Disclosing your Personal Information

In line with modern business practices common to many financial institutions, and pursuant to your specific needs (such as where you have a financial adviser) we may disclose your personal information to the organisations described below. Where your personal information is disclosed we will seek to ensure that the information is held, used or disclosed consistent with the Australian Privacy Principles, any other applicable privacy laws and codes.

The relevant organisations are those

- involved in providing, managing or administering your product or service such as third party suppliers, other FCC organisations, loyalty and reward program partners, printers, posting services, call centres, and our franchisees
- FCC organisations that wish to inform you of their products or services that might better serve your financial, business and lifestyle needs, or to notify you of promotions or other opportunities in which you may be interested, except where you tell us not to
- who are your franchisees and their service providers
- involved in maintaining, reviewing and developing our business systems, procedures and infrastructure including testing or upgrading our computer systems
- involved in a corporate re-organisation
- involved in a transfer of all or part of the assets or business of an FCC organisation
- involved in the payments system including financial institutions, merchants and payment organisations
- involved in product planning and development
- which are your representatives including your legal advisers
- as required or authorised by law, such as under the *Anti-Money or Laundering and Counter Terrorism Financing Act* 2006 (Cth) where you have given your consent.

In addition, for FCC organisations offering

- Finance products or services - other organisations to which personal information is usually disclosed are card producers, card schemes, credit and fraud reporting agencies, debt collection agencies, your guarantors, organisations involved in valuing, surveying, or registering a security property or which otherwise have an interest in such property, purchasers of debt portfolios, underwriters, re-insurers and other organisations involved in our normal business practices (such as securitisation)
- Trustee or custodial services - other organisations to which personal information is usually disclosed are superannuation and managed funds organisations, their advisers and other organisations involved in our normal business practices
- Other organisations to which personal information is usually disclosed are fraud detection agencies and other organisations involved in our normal business practices.

Your personal information may also be disclosed to other organisations involved in our normal business practices (such as securitisation) and used in connection with such purposes as outlined above.

Because we operate throughout Australia and overseas, some of these uses and disclosures may occur outside your State or Territory and/or outside of Australia, we will ensure the recipient complies with the Australian Privacy Principals and our privacy policy. In some circumstances we may need to obtain your consent before the recipient receives any personal information.

Credit-related information

We exchange credit-related information for the purposes of assessing your application for finance and managing that finance. If you propose to be a guarantor, one of our checks may involve obtaining a credit report about you.

This credit-related information may be held by us in electronic form on our secure servers and may also be held in paper form. We may use cloud storage to store the credit-related information we hold about you.

Notifiable matters

The law requires us to advise you of 'notifiable matters' in relation to how we may use your credit-related information. You may request to have these notifiable matters (and this policy) provided to you in an alternative form.

We exchange your credit-related information with credit reporting bodies. We use the credit-related information that we exchange with the credit reporting body to confirm your identity, assess your creditworthiness, assess your application for finance or your capacity to be a guarantor and manage your finance.

The information we can exchange includes your identification details, what type of loans you have, how much you have borrowed, whether or not you have met your loan payment obligations and if you have committed a serious credit infringement (such as fraud).

If you fail to meet you credit obligations or commit a serious credit infringement, FCC may undertake the following:

- Disclose repayment history information to a Credit Reporting Body.
- Issue prescribed notices under Credit Reporting Privacy Code advising payments which have become overdue more than 60 days.
- Issue prescribed notices under Credit Reporting Privacy Code a payment default has occurred with FCC advising a Credit Reporting Body.
- Engage Collections Agencies and or Legal Counsel to collect payments which have become overdue.
- Request a Credit Reporting Body not to disclose information about you if you believe you are a victim of fraud.

You have the right to request access to the credit-related information that we hold about you and make a request for us to correct that credit-related information if needed. Please see the heading 'Access and correction to your personal and credit-related information', below.

Sometimes your credit information will be used by credit reporting bodies for the purposes of 'pre-screening' credit offers on the request of other credit providers. You can contact the credit reporting body at any time to request that your credit information is not used in this way.

You may contact the credit reporting body to advise them that you believe that you may have been a victim of fraud. For a period of 21 days after the credit reporting body receives your notification the credit reporting body must not use or disclose that credit information. You can contact any of the following credit reporting bodies for more information:

- Equifax Pty Ltd – www.equifax.com.au,
- Dun & Bradstreet (Australia) Pty Ltd – www.dnb.com.au, or
- Experian Australia Credit Services Pty Ltd – www.experian.com.au.

Marketing our products and services

We may use or disclose your personal information to let you know about, and develop, products and services from across FCC that may better serve your financial, business and lifestyle needs, or to notify you of promotions or other opportunities in which you may be of interest to you. For example, we may do this after an initial marketing contact.

You can contact us at any time if you no longer wish us to do so (see Contacting Us below). If the direct marketing is by email you may also use the unsubscribe function. We will not charge you for

giving effect to your request and will take all reasonable steps to meet your request at the earliest possible opportunity.

Keeping your personal information accurate and up-to-date

We aim to make sure that the personal information we collect, use or disclose is accurate, complete and up-to-date and take reasonable steps to make sure this is the case. In this way we can ensure that we provide you with a better service.

If you believe your personal information is not accurate, not complete or not up to date, please contact us (see Contacting Us below). We will generally rely on you to ensure the information we hold about you is accurate or complete.

Access and correction to your personal and credit information

We will provide you with access to the personal and credit-related information we hold about you. You may request access to any of the personal information we hold about you at any time. We may charge a fee for our costs of retrieving and supplying the information to you.

Depending on the type of request that you make we may respond to your request immediately, otherwise we usually respond to you within seven days of receiving your request. We may need to contact other entities to properly investigate your request.

There may be situations where we are not required to provide you with access to your personal or credit-related information. Factors affecting a right to access include:

- access would pose a serious threat to the life or health of any individual
- access would have an unreasonable impact on the privacy of others
- a frivolous or vexatious request
- the information relates to a commercially sensitive decision making process
- access would be unlawful
- access would prejudice enforcement activities relating to criminal activities and other breaches of law, public revenue, a security function or negotiations with you
- legal dispute resolution proceedings
- denying access is required or authorised by or under law

An explanation will be provided to you, if we deny you access to the personal or credit-related information we hold about you.

If any of the personal or credit-related information we hold about you is incorrect, inaccurate or out of date you may request that we correct the information by contacting us by one of the methods referred to in the *Contacting Us* section of this document.

If appropriate we will correct the personal information at the time of the request, otherwise, we will provide an initial response to you within seven days of receiving your request. Where reasonable, and after our investigation, we will provide you with details about whether we have corrected the personal or credit-related information within 30 days.

We may need to consult with other finance providers or credit reporting bodies or entities as part of our investigation.

If we refuse to correct personal or credit-related information we will provide you with our reasons for not correcting the information.

Business without identifying you

In most circumstances it will be necessary for us to identify you in order to successfully do business with you, however, where it is lawful and practicable to do so, we will offer you the opportunity of doing business with us without providing us with personal information, for example, if you make general inquiries about interest rates or current promotional offers.

Protecting your personal information

Records of your personal information are kept in several forms including both paper and electronic form. The security of your personal information is important to us and we take all reasonable precautions to protect it from unauthorised access, modification or disclosure and from loss or misuse. These precautions include:

- confidentiality requirements for our employees
- document storage security policies
- security measures for systems access
- providing a discreet environment for confidential discussions
- only allowing access to personal information where the individual seeking access has satisfied our identification requirements
- access control for our buildings
- the security measures described below under Our Websites.

If FCC receives any personal information which we did not solicit the information, FCC will determine whether or not we could have collected the information if we had reasonably solicited the information. If not, we will take reasonable steps destroy this information.

Mandatory data breach reporting

FCC is required to comply with the Notifiable Data Breach (NDB) scheme from 22 February 2018.

Our data breach response plan provides the ability to respond quickly to any such breaches and includes:

(a) the steps and actions staff should take in the event of a breach or suspected breach;

(b) reporting lines if staff suspect a data breach;

(c) the recording of data breaches;

(d) means for identifying and addressing anything that contributed to the breach; and

(e) systems for a post-breach review and assessment of the entity's response to the data breach.

A data breach occurs when personal information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse.

What is an eligible data breach?

An eligible data breach warranting notification will arise when:

(a) there has been unauthorised access to or unauthorised disclosure of personal information; and
(b) access or disclosure would likely result in serious harm to affected individuals.

An eligible data breach can occur irrespective of the number of individuals that are likely to be at a risk of serious harm.

A determination of whether a data breach has or may cause serious harm will be dependent on the following factors:

(a) the sensitivity of the personal information which has been exposed due to the data breach;
(b) whether the information is protected by security measures and the likelihood that any such security measures could be overcome;
(c) who has or may have obtained or could obtain the information; and
(d) the nature of the harm, for example, whether any affected individuals will suffer financial or reputational damage.

Assessing a suspected data breach

If we suspect that an eligible data breach has occurred, we will take the following steps.

(a) Where possible contain the breach and take remedial action.
(b) Conduct a reasonable and expeditious assessment of the breach to determine whether notification is required. We will take all reasonable steps to complete our assessment within 30 calendar days after the day it first became aware of the suspected data breach.
(c) Where serious harm cannot be mitigated through remedial action, we will notify individuals at risk of serious harm and provide a statement to the OAIC as soon as practicable, but not later than 30 calendar days from becoming aware of the breach.

If it is not practicable to notify individuals at risk of serious harm, we will publish a copy of the statement prepared for the OAIC on our website, and take reasonable steps to bring its content to the attention of individuals at risk of serious harm.

The Data Breach plan is regularly reviewed and tested by the Compliance Officer

Complaints Handling

Any Complaints are required to be submitted in writing to FCC, as required by S40(1A) of the Privacy Act.

On receipt of a complaint by a company, business or individual, it must relate to an act or practice of FCC and we must:

- within 7 days after the complaint is made, acknowledge receipt of the complaint
- investigate the matter via the FCC's Disputes & Complaints Resolution Policy, make a decision and advise the company, business or individual within 30 days.
- set out the decision and indicate if you are dissatisfied with FCC's response, you can refer the complaint to the Office of Australian Information Commissioner www.oaic.gov.au

Your privacy on the Internet

Our Websites

We take care to ensure that the personal information you give us on our websites is protected, with electronic security systems in place, including the use of firewalls and data encryption. Depending on the FCC organisation with which you deal, user identifiers, passwords or other access codes may also be used to control access to your personal information. Please refer to the website of those FCC organisations with which you transact electronically for more information on our website specific privacy and security procedures.

Links to Other Sites

You may be able to access external websites by clicking on links we have provided. Those other websites are not subject to our privacy standards, policies and procedures. You will need to contact or review those websites directly to ascertain their privacy standards, policies and procedures.

Using Government Identifiers

Although in certain circumstances we are required to collect government identifiers such as your Medicare number or drivers licence details, we do not use or disclose this information other than when required or authorised by law, or unless you have voluntarily consented to disclose this information to any third party.

Your sensitive information

Without your consent we will not collect information about you that reveals your racial or ethnic origin, political opinions, religious or philosophical beliefs or affiliations, membership of a professional or trade association, membership of a trade union, details of health, disability, sexual orientation, or criminal record.

This is subject to some exceptions including when:

- the collection is required by law
- has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to FCC's functions or activities has been, is being, or may be engaged in the information is necessary for the establishment, exercise or defence of a legal claim.

Resolving your privacy issues

If you have any issues you wish to raise with the FCC, or would like to discuss any issues about our Privacy Policy, then you are able to do so by Contacting Us using our contact details at the end of this document.

Unsubmitted on-line applications.

If you start but do not submit an on-line application, FCC may contact me/us using any of the contact details you supply, to offer help completing it. If you do not submit the on-line application, the information in it will be kept by FCC for a period of time before being destroyed.

Contacting Us

At FC Capital we care about your privacy and your trust is important to us.

Should you have any queries or concerns about your privacy, please provide full details the nature of your concerns by contacting the FC Capital Privacy Officer, care of any of the following details:

Phone: +1800 307 903

Fax: +61 2 8458 0704

Email: privacy@firstclasscapital.com.au

Post: Privacy Officer, PO Box H173, Australia Square Sydney 1215