FIRST ACCESS FUNDING CORP. – PRIVACY POLICY

The Ten Privacy Principles of First Access Funding

First Access Funding Corp. and its subsidiaries and affiliated entities, if any, and their respective representatives (collectively "**First Access**") have always been and will continue to be committed to maintaining the accuracy, confidentiality, and security of your personal information. As part of this commitment, we have established our Ten Privacy Principles to govern our activities as they relate to the use of client personal information. We invite you to review our principles, which have been built upon the values set by Canada's federal Personal Information Protection and Electronic Documents Act ("**PIPEDA**").We may amend this privacy policy from time to time to reflect changes in the regulatory environment and/or industry practices and standards and will post any such revised policy on our website at www.fafcorp.ca. This privacy policy was last updated on February 1, 2016.

Principle One	-	Accountability
Principle Two	-	Identifying Purposes
Principle Three	-	Consent
Principle Four	-	Limiting Collection
Principle Five	-	Limiting Use, Disclosure and Retention
Principle Six	-	Accuracy
Principle Seven	-	Safeguarding Client Information
Principle Eight	-	Openness
Principle Nine	-	Client Access
Principle Ten	-	Handling Client Complaints and Suggestions

Principle One — Accountability

First Access is responsible for personal information under its control. In fulfilling this mandate, we have designated an individual or individuals who is/are accountable for compliance with our Ten Privacy Principles.

Principle Two — Identifying Purpose

The purposes for which personal information is collected, used and disclosed are to be identified before or at the time we collect personal information. First Access complies with this principle by, among other steps, making available this privacy policy to all affected individuals.

Principle Three — Consent

The knowledge and consent of the client are required for the collection, use or disclosure of client personal information, except where inappropriate or permitted by law. Depending on the sensitivity of the information, this consent can be implied or expressed; however, wherever commercially feasible First Access shall attempt to obtain express consent. First Access complies with this principle by, among other steps, structuring its Sales Contracts (including the Disclosure Statement and Agreement for Installation component) to provide easily accessible and understandable consent language. Consent to our use of personal information can be withdrawn at any time by following the directions at the end of this policy; however, a client may not withdraw his or her consent following an application for a First Access product or service for which credit worthiness verification is a prerequisite.

Principle Four — Limited Collection

Client personal information collected must be limited to those details reasonably necessary for the purposes identified and must be collected by fair and lawful means. Accordingly, First Access neither collects information which pertains to client health, race or ethnic origin.

Principle Five — Limiting Use, Disclosure and Retention

Client personal information may only be used or disclosed for the purpose for which it was collected unless the client has otherwise consented, or when it is required or permitted by law. As client personal information is only to be retained for the period of time required to fulfill the purpose for which it was collected First Access has established and implemented guidelines and procedures for retaining and destroying such information.

Principle Six — Accuracy

Client personal information, as available to us, shall be maintained in as accurate, complete and up-to-date form as is necessary to fulfill the purpose for which it is to be used. If any of your information changes please inform us by contacting us as described at the end of this privacy policy so that we can make any necessary changes.

Principle Seven — Safeguarding Client Information

Client personal information must be protected by security safeguards that are appropriate to the sensitivity level of the information. For example, Sales Contracts are kept in cabinets within the applicable office that are kept locked after business hours to avoid/prevent unauthorized access. All First Access computer systems are password protected for this same reason.

Principle Eight — Openness

We are required to make specific easily understandable information available to clients concerning the policies and practices that apply to the management of their personal information. Making available to clients this privacy policy, via our website, is a key method of making such information available.

Principle Nine — Client Access

Upon request, a client shall be informed of the existence, use and disclosure of their personal information, and shall be given access to it. Clients may verify the accuracy and completeness of their personal information, and may request that it be amended, if appropriate. Contact us as described at the end of this privacy policy. Summary information is available on request and we will respond to the request within 30 days of receipt. More detailed requests which require archive or other retrieval costs may be subject to our normal professional and disbursement fees and may take longer to respond to.

Principle Ten — Handling Client Complaints and Suggestions

Clients may direct any questions or enquiries with respect to the privacy principles outlined above or about our practices by contacting the designated person(s) accountable for privacy.

Why is personal information needed?

We collect, use and disclose client personal information in order to:

- confirm client identity;
- assess client suitability for our financial products and services;
- provide the financial products and services that have been requested or to offer additional products and/or services we believe the client may be interested in;
- communicate with clients;
- process account payments and/or transactions;
- communicate accurate information to credit reporting agencies;
- meet regulatory requirements, including compliance with privacy laws; and
- respond to any event(s) of default.

What is collected?

"Personal information" is any information that identifies a client, or by which a client identity could be deduced. Please note that "personal information" does not include either aggregate information that does not allow an individual to be identified, information about a visit to our website(s) which is not linked to the client, information about a client's computer operating system and web browser software (this technical information is verified to ensure that our website(s) are optimized to serve our clients) or, information that is used for the purpose of communicating or facilitating communication with an individual in relation to their employment, business or profession. We use anonymous/non-personal information to improve our products and services to our clients.

We only collect non-prohibited personal information which is related to our business such as client name, address, date of birth, social insurance number and employment information. We collect social insurance numbers as they provide the most reliable basis for us to conduct

accurate searches of credit rating databases. We likely will also require information about client income, assets and liabilities. If applicable, we will collect GPS based locations information via the consent to installation of a device in the client's vehicle.

How is personal information collected?

Wherever possible we collect personal information in an active fashion directly from the client. Please note that we may elect to record a conversation with a client for quality control and accuracy purposes.

Sometimes we may obtain information about clients from other sources for example:

- from a credit reporting agency;
- from other reported income sources;
- from client provided personal and professional references;
- from our automotive dealership partners; and
- passively by recording data on the history of a client's acquisition of services from First Access.

Will information be disclosed to outside parties?

First Access does not disclose your personal information to any third party to enable them to market their products and services. We are obliged to keep client personal information confidential except under the following circumstances:

• when expressly or impliedly authorized by the client, for example disclosures to credit reporting agencies and other organizations in order to verify that the personal information provided by a client is accurate as well as for credit approval purposes – please note that in certain limited circumstances when the services we are providing to you requires us give your information to third parties your consent will be implied, unless you tell us otherwise.

• when we are required or authorized by law to do so, for example if a court issues a subpoena;

• if we engage a third party to provide products and/or services to us (like computer back-up services or archival file storage) and such third party is contractually bound by our privacy policy and all applicable privacy laws, please note that such service provider(s) may be located outside of Canada;

• personal information located outside of Canada may result in the information being subject to foreign access requests;

• if we sell a portion of all of our business to a third party that will continue to provide the service(s) formerly provided by First Access;

• when we share such information with our subsidiaries or affiliated companies;

• where it is necessary to establish or collect fees; or

- if the information is already publicly known.

How is personal information safeguarded?

We implement commercially reasonable industry standard policies, procedures, technologies and security standards to ensure that client personal information is protected against unauthorized access, and inappropriate disclosure, alteration or misuse. All safety and security measures which are implemented are designed to be appropriate to the sensitivity level of the stored client personal information. Among the steps taken to protect your information are:

- premises security;

- restricted file access to personal information to only those with a need to know;

- deploying technological safeguards like security software and firewalls to prevent hacking or unauthorized computer access;

- internal password and security policies;

- secure disposal of personal information no longer needed; and

- screening and training of personnel.

First Access cannot, however, guarantee that loss, misuse or unauthorized use will never occur (for example, someone could conceivably overcome our security measures). If you receive any electronic communication which purports to be from First Access that you have any questions or concerns about, please contact us. Spam, improper use, and pirating of domain names and email addresses is a growing problem, so we appreciate hearing about incidents in order that we may investigate them and provide you the best client service.

Can access to personal information be denied?

Rights to access personal information are not absolute. We may deny access to a client when:

- denial of access is required or authorized by law;

- information relates to existing or anticipated legal proceedings against the client;

- the information was generated as a result of a formal dispute resolution process including a court case; or

- when granting the client access would have an unreasonable impact on other people's privacy, security or proprietary information.

If we deny a request for access to, or refuse a request to correct information, we shall do so in writing and explain why.

Communicating with us

Any channel of communication, such as e-mail, is not 100% secure, and you should be aware of this when contacting us to send personal or confidential information. With respect to Canada's Anti-Spam Legislation (commonly referred to as CASL), clients hereby expressly consent to receiving, during and after our business relationship, electronic messages from First Access, including via emails and through social media, providing information to you including newsletters, updates, alerts, other publications, news and communications, other information of interest to you and/or information on our services. You can withdraw this consent or modify your preferences as to the types of electronic messages which you wish to receive from us, at any time, simply by notifying us or by using the unsubscribe mechanism on any of our electronic messages.

How to file a complaint?

First Access has a privacy officer who may be contacted to answer any comments or questions about this privacy policy. Please forward your written communication to:

Telephone: 1-888-816-5574

E-mail: privacy@fafcorp.ca

Address: 10109-106 Street
Edmonton, Alberta
T5J 3L7

Attention: Privacy Officer

If you are not satisfied with our response, the Office of the Privacy Commissioner of Canada which oversees PIPEDA can be reached at:

Place de Ville

112 Kent Street, 3rd Floor

Ottawa Ontario, K1A 1H3

1-800-282-1376

www.privcom.gc.ca