Frontier Advisors Privacy Policy

August 2017

Respecting your privacy

Frontier Advisors Pty Ltd ACN 074 287 406 of Level 16, 222 Exhibition Street, Melbourne, Victoria, Australia 3000, and our subsidiaries and related bodies corporate ("we", "our" and "us") are committed to supporting the "Australian Privacy Principles" ("APPs") contained in the Privacy Act 1988 (Cth) ("Privacy Act").

Our respect for your right to privacy of your personal information is paramount. We ensure that all personal information, no matter how or where it is obtained, is handled in accordance with the APPs.

This Privacy Policy sets out:

- matters of which you should be aware regarding information we may collect about you;
- our policies on the management of your personal information; and
- generally, what sort of information we hold, why we hold the information we hold, and how we collect, hold, use and disclose that information.

You may not provide us with personal information or you may deal with us on an anonymous or pseudonymous basis. However, this may restrict our ability to provide our services to you or to otherwise deal with you (including responding to requests for access to or correction of your personal information or responding to a complaint).

Terminology

In our Privacy Policy, "personal information" refers to information or an opinion about an identified person or a person who is reasonably identifiable from the information or opinion.

How do we collect your personal information?

In accordance with the APPs, we only collect personal information about an individual if the information is necessary for one or more of our functions or activities and we must only collect personal information by lawful and fair means. Further, we must not collect personal information in an unreasonably intrusive manner. If it is reasonable and practicable to do so, we will collect personal information about an individual only from that individual. However, we comply with the APPs by taking reasonable steps to make an individual aware of the matters outlined in our Privacy Policy, even where we collect the personal information about an individual from someone else.

We may collect your personal information directly from you, or alternatively where permitted under the APPs, from third parties. Sources may include, but are not limited to:

- your employer in the case of being authorised to use our Partners Platform online portal;
- Partners Platform online portal usage data;
- a telephone or in-person inquiry about our services;
- emails or other electronic means (including by using our website);
- third parties, such as credit reporting agencies or your representatives;

- publicly available sources of information; and
- our service providers.

The types of personal information we may collect includes (but may not be limited to) your name, address, telephone number, email address and photographs.

We may also collect "de-identified information" about you through your use of our website for statistical purposes, including the dates and times you access our website, the domains from which you visit our website, your activity on our website and Internet Protocol addresses. This information is referred to as "click stream data" and we may use this data to analyse trends and statistics in order to improve our website and our services. This information is usually anonymous and we do not use it to identify individuals. However, due to the nature of internet protocols, such information might contain details that identify you. We collect this data using various technologies, including "cookies". A "cookie" is a text file that our website sends to your browser which is then stored on your computer as an anonymous tag identifying your computer (but not you) to us. You can set your browser to disable cookies. However, some parts of our website may not function properly or at all if cookies are disabled.

Some pages on our website and emails created by our website may also contain a "web beacon". A web beacon is a clear-pixel image which enables us to monitor your Internet activity on our website. When you view a page containing a web beacon, a de-identified notice of your visit is generated which we may process. A web beacon generally works in conjunction with a cookie. If a person disables cookies, a web beacon will be able to generate an anonymous notice of the visit but which cannot be associated with the information contained in a cookie.

How do we store your personal information?

We store your personal information on a server based in Australia using all reasonable security measures to prevent unauthorised access to or disclosure of your personal information. We also take all reasonable measures to destroy or permanently de-identify personal information when it is no longer required. The nature of the measures we take depend on the type of information, how the information is collected and how we store the information.

Why do we collect your personal information?

We may collect personal information for one or more of the following purposes:

- to provide our services to you or to other persons or organisations that are related to you;
- to provide you or any other person or organisation related to you with access to our online portal;
- to market, advertise or otherwise promote our services;
- to undertake market research in relation to our services;
- to improve our website, our online portal and our online services; and
- to comply with our obligations under any applicable laws.

We may need your personal information to notify you of our future improvements to our services or to seek your participation (purely on a voluntary basis) in advertising campaigns, launches, customer testimonials and focus groups.

Generally, you have no obligation to provide any information we request (save under any contract between you or your related party and us where you may be obliged to provide information). If you choose to withhold requested information, however, we may be unable to provide you or other persons or organisations that are related to you or which you represent with the services that depend on our collection of your personal information (particularly if the collection of that information is required by law).

Where we use your personal information to directly market ourselves or our services to you and we collected this information directly from you, we will use your personal information to directly market to you where you would reasonably expect us to use your personal information for that purpose. Where we collect your personal information from other sources, we will first obtain your consent in accordance with the Privacy Act.

How do we use and disclose your personal information?

We generally use your personal information to provide goods or services to you or to other persons or organisations related to you or which you represent. For example, we need your contact details to provide you with access to our investment advisory services (including via our online portal).

We may disclose your personal information to third parties (including credit reporting agencies, banks and our professional advisers) for the purpose of completing our obligation owed to you or any entity associated with you under any contract between us and you or such entity, as required by law. We may disclose your personal information, with your consent or otherwise in compliance with the Privacy Act, to our overseas partners in the Global Investment Research Alliance.

We may use or disclose your personal information for the purpose of directly marketing our services to you. We may use your personal information for the purpose of verifying your identity and responding to your requests for access to and/or correction of your personal information we hold, and responding to and handling any complaints you may have regarding our use and/or disclosure of your information.

You have the right to tell us that you do not want us to send information to you other than for the main purpose for which we collect your personal information. Where possible, we try to ensure that our disclosure of your personal information to other organisations is in a way which does not personally identify individuals.

How do we protect your personal information?

We take reasonable steps to protect your personal information which we hold from misuse and loss and from unauthorised access, modification or disclosure.

When using our website or our online portal, you should be aware that no data transmission over the Internet can be guaranteed to be totally secure. We do not warrant the security of any information transmitted over the Internet, although we strive to protect such information. By using our website and our online portal, you accept that your information will be transmitted to and from our website and portal at your own risk.

Destruction of your personal information

Where permitted by law, if we no longer need your personal information for any purpose outlined above, we will take reasonable steps to destroy or permanently de-identify your personal information.

Access to and correction of your personal information

In accordance with the APPs, we will provide you with access to any of your personal information we hold, unless the request is unreasonable or the Privacy Act or the APPs permit or require us to decline that request. If you wish to access personal information we hold about you, please write to us at Frontier Advisors Pty Ltd, Level 16, 222 Exhibition Street, Melbourne, Victoria, Australia 3000. You may also email us at mail@frontieradvisors.com.au.

Of course, before we provide you with access to your personal information we will require you to verify your identity to us.

For most requests, access to your personal information will be provided free of charge. However, we may charge a reasonable fee if your request requires a substantial effort on our part.

If you need to update your information (i.e. if you change your address), please contact us so that we can make the change.

Complaints

If you wish to make a complaint about an alleged breach of your privacy or an alleged breach of the APPs, the complaint should be made in writing to the address or email address listed above.

Receipt of your complaint will be acknowledged and we will endeavour to deal with your complaint and provide you a response within a reasonable time following our receipt of your complaint (which in most situations will be within 30 days of our receipt of your complaint). Where a matter requires a more detailed investigation it may take longer to resolve. We will provide you with progress updates if this is the case and may seek further information from you.

Where required by the Privacy Act, we will provide written acknowledgment of your complaint and information on how we will deal with your complaint. Further, where we are required to do so by the Privacy Act, we will provide you in writing our determination on your complaint.

We may refuse to investigate and deal with a complaint if it is considered to be vexatious.

If you are dissatisfied with the outcome of your complaint, you may seek internal review of the decision. Internal review will be conducted by an officer who has not previously been involved in your complaint.

If you are still dissatisfied with the outcome of your complaint, you are also able to take your complaint to an external dispute resolution provider (in the case of a complaint in relation to credit-related personal information) that applies to us and/or the Office of the Australian Information Commissioner for resolution.

Data Breach Notification Requirements

Effective 23 February 2018, the Privacy Act will require us to report "eligible data breaches" to the Office of the Australian Information Commissioner and to affected individuals.

An "eligible data breach" occurs if there is unauthorised access to, or disclosure of, information we collect and a reasonable person would conclude that such access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates. “Serious harm”, while undefined, is likely to include serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation.

An exception applies when remedial action is taken to prevent serious harm to any affected individual before the individual suffers the harm. If the breach applies to multiple entities, only one entity must notify the Office of the Australian Information Commissioner and affected individuals for all entities. Reporting is not required if it would be likely to prejudice law enforcement related activity or it would be inconsistent with a secrecy provision.

We must take reasonable steps to notify affected individuals of the breach, such as via email, telephone or post. However, if we determine that it is not practicable to notify affected individuals directly, then we must publish a statement on our website and take reasonable steps to publicise the statement.

Updates to our Privacy Policy

We may amend or replace our Privacy Policy from time to time. Any changes to this Privacy Policy will be published on our website.

You may obtain a copy of our current Privacy Policy from our website or by contacting us using the contact details set out above.