Zebra Financial Services (ZFS) commitment to protecting privacy

ZFS is committed to protecting the personal information of clients in accordance with the Australian Privacy Principles under the *Privacy Act 1988* (Cth) ('Act'). The ZFS Privacy Policy Statement contains information about our privacy practices. A copy of this Statement can be accessed via the website at www.montrefinancial.com.au.

Personal Information

Personal information is any information or opinion about an identified individual, or an individual who is reasonably identifiable. This can be whether the information or opinion is true or not and whether the information or opinion is recorded in material form or not. Examples include anything from a name, a photo, an email address, bank account details, posts on social networking websites, medical information, or a computer IP address.

Data Breaches

An eligible data breach occurs when three criteria are met:

- There is unauthorised access to, or unauthorised disclosure of personal information, or a loss of personal information that an entity controls or has possession over. This could be by an employee, an independent contractor or a third party (i.e. hacking);
- This is likely to result in serious harm to one or more individuals or serious harm is more than probable to occur based on the perspective of a reasonable person, and
- You have not been able to prevent the likely risk of serious harm with remedial actions.

Serious Harm

Whether a data breach is considered to cause serious harm will be decided by the Risk & Compliance Officer and will be made based on the information immediately available or following reasonable inquiries or an assessment of the data breach.

Serious harm is not defined in the Privacy Act 1988 (Cth) however the Office of the Australian Information Commissioner (OAIC) provides guidance as to what will constitute serious harm. Serious harm may be physical, psychological, emotional, financial or reputational.

When considering the likeliness of serious harm, the following will be considered:

- The kind or kinds of information (documents commonly used for identity fraud including Medicare card, driver licence, financial information and passport details);
- The sensitivity of the information (such as information about a person's health, whether the information belongs to a minor);
- Whether the information is protected by one or more security measures (e.g. encryption or passwords); If the information is protected by one or more security measures – the likelihood that any of those security measures could be overcome,
- The persons, or the kind of persons, who have obtained, or could obtain, the information;
- If a security technology or methodology was used in relation to the information, and was designed to make the information unintelligible or meaningless to a person who is not authorised to obtain the information;

- The likelihood that the persons, or kind of persons, who have, or are likely to have, the intention of causing harm to any individuals to whom the information relates and have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology;
- The nature of the harm, and
- Any other relevant matters.

What To Do

In the event of a breach the following two steps are critical:

1. **Contain the Data Breach** - Contact the Risk and Compliance Officer immediately for advice on the steps to undertake to remediate a suspected or known breach. This is to ensure that any remedial action taken does not exacerbate the breach. This will involve the business taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of the information and following up that this attempt has been successful. An example of remedial action might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised access can occur.

   If there is still some risk of serious harm after taking remedial action to a group or to certain individuals affected within a group the remedial action will be deemed to be insufficient; and further notification to the Commissioner will be required.

2. **Assess the Data Breach** – The Risk and Compliance Officer will review and assess the breach and consider:

   - Whether the data breach is likely to result in serious harm to any of the individuals whose information was involved.
   - If on reasonable grounds it is believed that serious harm has resulted, then notification to the OAIC and the client will be required by the NDB Act.
   - If there are not grounds to suspect that serious harm may have resulted, then the Risk and Compliance Officer will conduct an assessment and investigate how to ensure the breach does not occur again.

Note: The OAIC expects that the amount of time and effort and entity will expend in an assessment should be proportionate to the likelihood of the breach and its apparent severity.

Notifiable Data Beach (NDB)

The Notifiable Data Breach scheme (established Feb 2018) includes the obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm.

The OAIC website has the appropriate NDB form which includes the following:

- Date and time of the discovery of the breach/suspected breach;
- Date and time of when the breach/suspected breach occurred;
- The type of personal information involved;
- The cause and extent of the breach and context of the affected information,
- List of affected individuals or those who have possibly been affected; and
- Whether there has been any attempt at remediation or if the action has been taken, when and by whom.

Where serious harm is likely, ZFS will notify the OAIC using the NDB form and notify the affected organisations and individuals and inform them of the details of the information that was provided to the OAIC.

Additionally, The Risk and Compliance Officer will consider whether it is necessary to report the incident to other relevant bodies such
as:

- Police or law enforcement;
- ASIC, APRA or the ATO;
- The Australian Cyber Security Centre; and
- Other relevant professional bodies.

A **Data Breach Response Summary Diagram** (provided by OAIC) is attached to this policy and provides an overview of a typical data breach response, including the requirements of the NDB scheme.

Prevention of Future Breaches

A review into the incident is to be taken and action to prevent future breaches put in place. This may include:

- fully investigating the cause of the breach,
- developing a prevention plan,
- conducting audits to ensure the plan is implemented,
- changes to your policies and business procedures, and staff training practices.

The ZFS Privacy Notice

Under the Act*, ZFS* is required to notify clients of certain privacy matters around the time of collecting their information. These matters are set out in the *ZFS Privacy Notice* which is embedded in this communication.

It is assumed that clients have read the *ZFS Privacy Notice* and have no objection to ZFS handing their personal information in the manner set out in the notice, however best practice would be to remind clients of this fact and talk through any questions the clients may have.

The ZFS Privacy Notice

Zebra Financial Services (ZFS) has always valued the privacy of personal information. When ZFS collect, use, disclose or handle personal information, ZFS will be bound by the *Privacy Act 1988* (Cth) (the 'Act').

Why do we collect your personal information?

ZFS collects personal information to offer, provide, manage and administer the many financial services and products we are involved in. These include insurance advice and claims management, superannuation and investment advisory services. ZFS may also collect personal information to be able to identify products and services that may interest you.

ZFS may collect information about you because we are required or authorised by law to collect it. There are laws that affect the provision of our many services and products which require us to collect certain personal information. These laws may include the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), the *Corporations Act 2001* (Cth), the *Superannuation Industry (Supervision) Act* 1993 (Cth) and the *Insurance Contracts Act 1984* (Cth).

How do we collect your personal information?

Unless impracticable or unreasonable to do so, ZFS will generally collect this information directly from you or your agents or we may collect it from third parties such as our affiliates or employers, insurance companies, insurance brokers or agents, credit organisations, motor vehicle and driver licensing authorities, financial institutions, medical professionals, third parties who may be arranging insurance cover for a group that you are a part of, law enforcement, dispute resolution, statutory and regulatory bodies, marketing lists and industry databases, publicly available sources etc. Upon your request, we will take reasonable steps to let you know of how we have sourced your personal information unless it is obvious from the circumstances that you would know or would reasonably expect us to have the information (such as where we are dealing with your advisors).

When you give ZFS personal information about other individuals, we rely on you to have made or make them aware that you will or may provide their personal information to us, the types of third parties we may provide it to, the relevant purposes we and the third parties we disclose it to will use it for, and how they can access it. If it is sensitive information we rely on you to have obtained their consent on these matters. If you have not done either of these things, you must tell us before you provide the relevant information.

You can choose not to receive product and service offerings from us (including product or service offerings from us on behalf of our affiliates and business partners) or related bodies, by contacting our Privacy Officer on info@zebrafs.com.au or your ZFS representative.

What can happen if you don't provide us with your information?

If you do not provide the information we request, we or those involved with the provision of the service or product may not be able to provide the appropriate type or level of service product.

To whom can we disclose your personal information?

ZFS discloses personal information to third parties who we believe are necessary to assist us in providing

the relevant services and products to our clients or to enable them to offer their products and services to you. For instance, we disclose personal information to the relevant product provider and their representatives, our agents and contractors and related companies. We generally limit, however, the use and disclosure of any personal information provided by us to such third parties to the specific purpose for which it was supplied. Disclosure may also be made to government, law enforcement, dispute resolution, statutory or regulatory bodies, or as required by law.

In addition to our affiliates, we may also disclose personal information to third parties such as our contractors, agents and service providers when we outsource certain functions, including paraplanning and administrative support. Our affiliates and third parties may be based locally or they may be overseas including the Philippines. In these circumstances, ZFS will generally take reasonable steps to ensure we have contracts in place with such parties which prevent them from using or disclosing personal information for any purposes other than our own. We will also make every effort to ensure that we only have business dealings with third parties that value privacy and information security the same way as us. However, by providing us with your consent to collect your information in accordance with this Privacy Notice you acknowledge that we will no longer be required to take reasonable steps to ensure the overseas recipient's compliance with the Act in relation to the handling of your information and we will not be liable to you for any breach of any Australian privacy law by these overseas recipients under the Act or otherwise and, on this basis, you consent to such disclosure.

Storage of your information

Personal information is typically stored electronically on secure servers and may be stored in files within secure office premises. Security and privacy measures are in place to ensure the integrity of your personal information and to protect it from misuses, interference and loss, and from unauthorised access, modification or disclosure.

Where we hold information that we longer require for any purpose and it is not required to be maintained by Australian law, we will take reasonable steps to destroy the information or ensure that the information is unable to be identified.

How can I access and correct my personal information or resolve my privacy issues?

If you wish to seek access to or correct the personal information we collected or disclosed about you, please telephone or email your ZFS representative. If you wish to lodge a written complaint, please address it to the Privacy Officer at the following address:

Zebra Financial Services Pty Ltd
Suite 112 350 George Street
Sydney NSW 2000
Email: info@zebrafs.com.au

The Privacy Officer will respond to your complaint within 30 days of its receipt.

You may also contact the Privacy Officer via phone on +61 1300 175 995.

If, however, you feel that your complaint has not been resolved, then you can contact the Office of the Australian Information Commissioner via one of the following means:

Post: GPO Box 5218, SYDNEY NSW 2001
Email: enquiries@oaic.gov.au
Phone: 1300 363 992
Online: https://www.oaic.gov.au