

Sufficient non written consent

FORM OF NON WRITTEN CONSENT SUFFICIENT FOR ROLLING OVER OR TRANSFERRING BENEFITS

Date of issue: 31 January 2002

I, Senthamangalam Ganesan Venkatramani, General Manager, Diversified Institutions Division, Australian Prudential Regulation Authority, under paragraphs 4.12(2)(b) and 6.27B(b) of the *Superannuation Industry (Supervision) Regulations* (the “SIS Regulations”), DETERMINE that, for the purposes of regulation 4.12 and Division 6.4 of Part 6 of the SIS Regulations, consent, other than written consent, shall be sufficient if it is in accordance with the form described in the Schedule.

This determination commences to have effect on 1 July 2002.

Dated 31 January 2002

S.G.Venkatramani
General Manager
Diversified Institutions Division

[NOTE: Where:

- (1) an amount proposed to be rolled over:
 - (a) out of a regulated superannuation fund or an approved deposit fund is an eligible termination payment (within the meaning of subsection 27A(1) of the *Income Tax Assessment Act 1936*) (an “ETP”); or
 - (b) into a regulated superannuation fund or an approved deposit fund is a qualifying ETP (within the meaning of subsection 27A(12) of the *Income Tax Assessment Act 1936*); and
- (2) the taxpayer wishes to utilise a trustee’s arrangement under this determination to give non written consent to the rollover;

the taxpayer must give instructions to the payer of the ETP, in respect of the rollover, that are consistent with both:

- (3) Subdivisions 3, 3A and 3B of Division 2 of Part 7 of the *Income Tax Regulations*; and
- (4) this determination.]

SCHEDULE

Interpretation

- (a) “consent” means a member’s consent or authority, given to the trustee of the fund out of which, or into which, the member’s benefits are rolled over or transferred;
- (b) “convey” means transmitted orally, electronically, or by any other means not in writing, and “conveyed” has a corresponding meaning;
- (c) “default arrangement” means an arrangement that states how, if insufficient or incorrect instructions are received by the trustee with respect to a rollover or transfer, the trustee will deal with the amount;
- (d) “electronic” includes, but is not limited to, transmission by computer, facsimile, optical or similar technologies, and “electronically” has a corresponding meaning;

Sufficient non written consent

- (e) “fund” means a regulated superannuation fund or an approved deposit fund;
- (f) “identifier” means a unique identifier allocated to a member by a trustee under item 2 of this Schedule, other than a Tax File Number, which may be, for example:
 - (i) a number or group of numbers; or
 - (ii) a password;that is capable of being conveyed to the trustee by non written means;
- (g) “member” means:
 - (i) a member of a regulated superannuation fund; or
 - (ii) a depositor in an approved deposit fund;who makes a transaction;
- (h) “transaction” means a rollover or transfer of a member’s benefits out of or into a fund where the member gives their non written consent using the identifier given to that member by the trustee under item 2 of this Schedule; and
- (i) “trustee” means the trustee of a fund.

This Determination replaces a previous Determination on this subject dated 30 June 1998.

Consent may be transmitted electronically, orally or in any other non written form, if, and only if, the procedure set out below is followed by the trustee in obtaining that consent.

- (1) Prior to an identifier, which meets the conditions set out under item 2, being used in a transaction, the trustee shall give the member a document, comprising binding conditions of use (the “conditions”), setting out the respective rights and obligations of the trustee and the member with respect to a transaction, including:
 - (a) that the member shall not be liable for any losses arising from:
 - (i) fraudulent or negligent conduct of the trustee’s employees or agents in relation to a transaction; and
 - (ii) the trustee’s system or equipment malfunctioning, including non-completion of transactions and unreasonable delays in carrying out the member’s valid instructions; and
 - (iii) any unauthorised transaction where the member has not contributed to such a loss; and
 - (iv) any unauthorised transaction occurring after the member has notified the trustee that the security of the member’s identifier has been breached; and
 - (b) subject to paragraph (c), how any other losses will be reasonably allocated between the trustee and the member, based on each party’s contribution to the loss; and
 - (c) except in the case of the member’s fraudulent conduct in relation to a transaction, placing a maximum limit on the member’s liability for the loss, which must in no circumstances exceed the total amount of the member’s benefits in the fund; and
 - (d) describing any default arrangement that the trustee has in place.
- (2) The trustee shall allocate an identifier to the member that is:

Sufficient non written consent

- (a) unique to the member; and
 - (b) capable of being solely held by, and confidential to, the member; and
 - (c) capable of verification by the trustee against its records.
- (3)** A transaction can only be validly made:
- (a) after the member has properly conveyed his or her non written consent using the identifier; and
 - (b) after the identifier has been verified against the trustee's records; and
 - (c) after the member has been informed, at the time of the transaction, of any default arrangement that may apply to the transaction; and
 - (d) if the transaction is accurately recorded by the trustee (whether electronically or otherwise) in a form capable of being readily accessed and understood at any time during the period which records are required to be kept by or under law. The trustee must take reasonable steps to protect the information it holds from misuse and loss and from unauthorised access, modification or disclosure.
- (4)** To avoid doubt, if the trustee alters any of the conditions after giving them to the member (including implementing a default arrangement for the first time, or changing an existing default arrangement) the trustee must notify the member as soon as is practicable (but need not allocate a replacement identifier to the member).

Sufficient non written consent

EXPLANATORY STATEMENT ACCOMPANYING DETERMINATION FOR THE PURPOSES OF SETTING OUT THE FORM OF NON WRITTEN CONSENT SUFFICIENT FOR ROLLING OVER OR TRANSFERRING BENEFITS

Superannuation Industry (Supervision) Regulations (the ‘SIS Regulations’) 4.12(2) and 6.27B allow for consent other than written consent, the form of which is determined by the Australian Prudential Regulation Authority (APRA) as sufficient in the circumstances, for, respectively:

- the acceptance by a regulated superannuation fund or approved deposit fund (ADF) of a rollover or transfer of benefits from another regulated superannuation fund or ADF or from a Retirement Savings Account (RSA); or
- the rollover or transfer of benefits from a regulated superannuation fund or ADF.

APRA has determined forms of non written consent in this Determination (which replaces a previous Determination on this subject dated 30 June 1998).

The usage of non written consent is optional. It is for the fund’s trustee to decide whether the circumstances of the fund are such that providing for non written consent for rollovers or transfers is viable or desirable. If a trustee chooses to accept non written consent to such transactions the Determination **must** be complied with. If, however, the trustee decides not to use non written methods of consent, then there is no need to for the Determination to be followed.

The object of this Determination is to set out the factors which will ensure sufficiency of the non written consent. The requirements set out in this Determination are not intended to regulate forms of non written consent on a detailed level, but are designed to ensure that non written forms of consent meet functions usually met by written forms of consent.

Background

Generally, under the SIS regulations, a member’s benefit in a regulated superannuation fund or an approved deposit fund cannot be rolled over or transferred unless the member has given consent.

Ordinarily, under the SIS regulations, the trustee of a regulated superannuation fund or an approved deposit fund cannot accept a transferred benefit unless consent has been given by the member, or the trustee reasonably believes it has been given.

Under the SIS Regulations, consent may be written or in any other form as determined. The Determination sets out the allowable form of the non written consent. It applies to, but is not limited to, consent transmitted electronically, oral consent, and other forms of non written consent such as PIN numbers using a telephone key pad.

It should be noted that, under Section 25 of the *Acts Interpretation Act 1901* any mode of representing or reproducing words, figures, drawings or symbols in a visible form is considered as writing. Therefore, the Determination does not cover consent given in this manner.

The Determination complements the *Income Tax Assessment Act (ITAA)* and Regulations, which aim to provide for electronic commerce and increased diversity of administration in the superannuation system.

Sufficient non written consent

The Determination

The Determination comes into force on 1 July 2002. It consists of four clauses that outline the elements with which non written consent to rollover or transfer of benefits must comply if that consent is to be regarded as sufficient. Key terms used in the Determination are also defined.

A form of consent to a rollover or transfer, which is not in writing, will only be regarded as sufficient if it meets the requirements set out in the Determination.

The Determination does not direct which types of technology or methods are preferred, but rather seeks to identify what is achieved by written consent, and then ensure that non written consent also performs these functions.

The Determination aims to achieve a balance between protecting members and allowing scope for technological advances to be incorporated into the superannuation system.

Clause 1 - Liability and Disclosure Arrangements

Due to the lack of traditional forms of identification (ie. written signatures) able to be used for verifying non written consent, the Determination imposes a requirement that an identifier must be issued by the trustee to the member and used in all non written transactions. Whenever an identifier is issued, members have a responsibility to act reasonably in safeguarding the identifier. Generally, there should be differing levels of member liability and/or trustee liability established depending on the degree of culpability or negligence involved in unauthorised use of the identifier or improper transactions, in accordance with the Determination where applicable.

Clause One provides that before a trustee allocates an identifier to a member to be used in non written consent transactions ('transactions'), legally enforceable conditions of use must be given by the trustee to the member setting out the rights and obligations with respect to transactions.

Clause One also sets out requirements relating to liability. Within these parameters the trustee can formulate conditions of use that are suitable to the fund's circumstances.

The following issues must be addressed in the conditions of use:

(a) that the member shall not be liable for any losses arising from:

As a means of providing protection for members, the Determination provides that in some circumstances members will not be liable for losses. Basically, the member will not be liable for loss which results from a transaction for which the member is not responsible, and to which the member has not contributed.

(i) fraudulent or negligent conduct of the trustee's employees or agents in relation to a transaction; and

Where a loss has occurred due to the fraud or negligence of the trustee's employees or agents, it would not be conscionable that the member be held liable, as they bear no responsibility for such losses.

(ii) the trustee's system or equipment malfunctioning, including non-completion of transaction and unreasonable delays in carrying out the member's valid instructions; and

Sufficient non written consent

The trustee is responsible for loss caused by the failure of the trustee's system or equipment. Such system or equipment malfunction may result in, for example, non-completion of a transaction or unreasonable delays in carrying out the member's valid instructions. If losses result from these circumstances, the member should not be liable as they are not responsible for causing the loss.

As the Determination aims to achieve media neutrality, an 'unreasonable delay' is best understood as being equivalent to a delay which would be considered unreasonable in a written consent environment.

(iii) any unauthorised transaction where the member has not contributed to such a loss; and

Where a member has not contributed to a loss which results from an unauthorised transaction, they should not be liable for any part of that loss.

(iv) any unauthorised transaction occurring after the member has notified the trustee that the security of the member's identifier has been breached; and

At the point in time where a member notifies the trustee that the security of their identifier has been breached, the trustee should immediately take steps to ensure that the identifier is no longer able to be used. The appropriate method to notify the trustee of a breach, such as calling the customer service telephone number, may be included in the conditions of use. The member should not be responsible for losses which occur after this time, as the trustee bears responsibility for ensuring that the compromised identifier is not accepted as a means of verification. If an identifier which has been reported as compromised is accepted at a later stage to authorise a non written transaction, the trustee is liable for any losses which occur.

(b) subject to paragraph (c), how any losses will be reasonably allocated between the trustee and the member, based on each party's contribution to the loss; and

As mentioned above, it is important that the liability for loss set out in the conditions of use be based on a fair allocation of responsibility. This is best achieved by ensuring that liability is allocated based on each party's contribution to the loss.

A member may be considered to have contributed to a loss where, for example, they have voluntarily disclosed their identifier; kept a record of the identifier (without making any reasonable attempt to disguise the identifier) in a place which is easily accessed by others in a manner which allows its purpose to be identified; or by committing other negligent acts which allow another person to access the member's account via a non written transaction.

When a member, through negligence, contributes to a loss they should, subject to the maximum liability limit provided for in (c), be liable for such a loss.

(c) except in the case of the member's fraudulent conduct in relation to a transaction, placing a maximum limit on the member's liability for the loss, which must in no circumstances exceed the total amount of the member's benefits in the fund; and

It is appropriate that the liability of the member differs according to the degree of culpability involved in the action which leads to the loss. It is reasonable that the member, except in cases of fraud, should not be liable for an amount which exceeds their total benefits in the fund. For

Sufficient non written consent

example, a member may act negligently in not safeguarding their identifier so that an unauthorised transaction occurs. However, if in carrying out the transaction the fund releases an amount which exceeds the benefits held by the member, then the fund should be liable for the amount of the loss which exceeds the member's benefits. Only in cases of fraud in which the member is involved is the member potentially liable for an amount in excess of their benefit.

(d) describing any default arrangement that the trustee has in place.

Due to the complexity of rollover and transfer transactions, situations may occur where instructions are not clear or cannot be carried out. In a case where insufficient instructions are received, the trustee is permitted to use a default arrangement, provided that the member is made aware of the arrangement, and its implications, through the conditions of use. Details of the default arrangement must also be advised to the member at the time of the non written transaction.

A default arrangement, in cases where insufficient or unclear instructions have been received from the member to enable the trustee to make the transaction, may consist of not progressing the transaction until the trustee has made contact with the member and received further information which is sufficient to complete the rollover or transfer.

The need to use the default arrangement may be ameliorated by seeking the necessary information in a structured manner eg. a stepped system where the instruction cannot be finalised until all steps are completed and all information is received and confirmed.

It should be noted that Regulation 99E of the ITAA, inserted by Statutory Rule No 14 effective 1 July 1998, provides that instructions must include information sufficient:

- to identify the amount and destination of any rollover payment; and
- to identify the amount of any cash amount; and
- to identify the tax components and preservation amounts of each rollover payment and cash amount; and
- to indicate how any 15 February 1990 rollover balance (if known) is to be distributed.

Clause 2 - Allocation of an Identifier

The identifier fulfils the functions of a written signature, including identifying the signer and allowing the signer to take a positive act to express approval and/or authorisation of the non written message. Any model of identifier and related delivery technology is acceptable provided it meets the requirements set out in the Determination.

A Tax File Number must not be used as an identifier.

Clause 2 provides that if the trustee proposes to accept non written forms of consent, the allocated identifier must be:

(a) unique to the member; and

Written signatures are regarded as legitimating transactions due to the fact that they are able, ideally, to uniquely identify the person who signs. In order for the allocated identifier to fulfil that function it must, be recognisable as unique to the individual member. Examples of a unique identifier are a PIN number, password etc.

Sufficient non written consent

(b) capable of being solely controlled by, and confidential to, the member; and

The identifier, to be capable of being relied upon as a safe and secure means of authenticating a transaction, must remain under the sole control of the member it is issued to. The trustee must take steps to ensure that the member is aware of the need and obligation to keep the identifier safe and confidential.

The liabilities under Clause 1 of the Determination also reflect the fundamental importance of ensuring the identifier's confidentiality.

(c) capable of verification by the trustee against its records.

For an identifier to fulfil the purpose of safeguarding a member's benefits and authenticating a transaction, it must be able to be verified. If an identifier is not able to be checked against a trustee's records and its authenticity thereby confirmed, it does not have value.

Clause 3 - Non written Consent Transactions - Necessary Elements

A non written transaction authorising a rollover or transfer of benefits is only able to be validly made on satisfaction of the following requirements:

(a) after the member has properly conveyed his or her non written consent using the identifier; and

As set out above, in a non written environment the use of an identifier that is unique, confidential and able to be authenticated is the primary means by which the legitimacy of a transaction can be assured. The identifier must be used for an instruction to be considered valid.

(b) after the identifier has been verified against the trustee's records; and

To ensure the legitimacy of the consent the identifier must be confirmed as that of the member before a valid transaction can be made. This is comparable to confirming a member's signature prior to acting on their instructions in a written environment.

(c) after the member has been informed, at the time of the transaction, of any default arrangement that may apply to the transaction; and

As provided for in Clause (1)(d), it may be necessary, due to the potential complexity of rollover and transfer transactions, to utilise a default arrangement where the instructions received from the member are insufficient or unclear for the trustee to carry them out.

The existence and operation of a proposed default arrangement must be disclosed to the member in the conditions of use, issued under Clause 1.

If any default arrangement applies, it must also be advised to the member at the time the member issues non written instructions. This reminder ensures that the member is aware of the default arrangement, and implications thereof, at the time of issuing the transaction instructions.

(d) if the transaction is accurately recorded by the trustee (whether electronically or otherwise) in a form capable of being readily accessed and understood at any time during the period which records are required to be kept by or under law.

Sufficient non written consent

When non written forms of consent are used, it is essential that adequate records of transactions are retained which are able to be accessed and reproduced in an understandable form. Such records should be held for a sufficient period of time to satisfy any legal requirements applicable to a fund's record keeping. If a trustee feels that it is appropriate that records are maintained beyond this time, it is, of course, open for them to do so. The trustee must take reasonable steps to protect the information it holds from misuse and loss and from unauthorised access, modification or disclosure.

As no form of record maintenance is prescribed, storage in electronic forms using decoding, compression, conversion of data, or by other means is permitted.

Clause 4 - To avoid doubt, if the trustee alters any of the conditions after giving them to the member (including implementing a default arrangement for the first time, or changing an existing default arrangement) the trustee must notify the member as soon as is practicable (but need not allocate a replacement identifier to the member).

The conditions of use, which, under Clause 1, the trustee must provide to the member prior to the allocation of an identifier, sets out the respective rights and obligations of the trustee and the member with respect to a non written transaction.

Where the trustee alters the conditions of use, the change must be notified to members as soon as is practicable. Such changes may include alterations to the default arrangement, or implementation of a default arrangement where none previously existed.

It is important that the member is notified of any change to the conditions of use as soon as practicable as the change may impact on the member's decision to utilise non written arrangements.

Any change to the conditions of use does not, however, void the original conditions, and it is not necessary for the member to be allocated a new identifier.

Dated 31 January 2002

(Published by authority of the Australian Prudential Regulation Authority)

Sufficient non written consent

FORM OF NON WRITTEN CONSENT SUFFICIENT FOR ROLLING OVER OR TRANSFERRING BENEFITS

Date of issue: 31 January 2002

I, Senthamangalam Ganesan Venkatramani, General Manager, Diversified Institutions Division, Australian Prudential Regulation Authority, under paragraph 4.30(b) of the *Retirement Savings Accounts Regulations* (the "RSA Regulations"), DETERMINE that, for the purposes of Division 4.4 of Part 4 of the RSA Regulations, consent, other than written consent, shall be sufficient if it is in accordance with the form described in the Schedule.

This determination commences to have effect on 1 July 2002.

Dated 31 January 2002

S.G.Venkatramani
General Manager
Diversified Institutions Division

[NOTE: Where:

- (1) an amount proposed to be rolled over:
 - (a) out of an RSA is an eligible termination payment (within the meaning of subsection 27A(1) of the *Income Tax Assessment Act 1936*) (an "ETP"); or
 - (b) into an RSA is a qualifying ETP (within the meaning of subsection 27A(12) of the *Income Tax Assessment Act 1936*); and
- (2) the taxpayer wishes to utilise an RSA provider's arrangement under this determination to give non written consent to the rollover;

the taxpayer must give instructions to the payer of the ETP, in respect of the rollover, that are consistent with both:

- (3) Subdivisions 3, 3A and 3B of Division 2 of Part 7 of the *Income Tax Regulations*; and
- (4) this determination.]

SCHEDULE

Interpretation

- (a) "consent" means an RSA holder's consent or authority, given to the RSA provider out of which, or into which, the RSA holder's benefits are rolled over or transferred;
- (b) "convey" means transmitted orally, electronically, or by any other means not in writing, and "conveyed" has a corresponding meaning;
- (c) "default arrangement" means an arrangement that states how, if insufficient or incorrect instructions are received by the RSA provider with respect to a rollover or transfer, the RSA provider will deal with the amount;
- (d) "electronic" includes, but is not limited to, transmission by computer, facsimile, optical or similar technologies, and "electronically" has a corresponding meaning;

Sufficient non written consent

- (e) “identifier” means a unique identifier allocated to an RSA holder by an RSA provider under item 2 of this Schedule, other than a Tax File Number, which may be, for example:
 - (i) a number or group of numbers; or
 - (ii) a password;that is capable of being conveyed to the RSA provider by non written means;
- (f) “RSA” has the same meaning as in the *Retirement Savings Accounts Act 1997*;
- (g) “RSA holder” means a person holding an RSA who makes a transaction;
- (h) “RSA provider” has the same meaning as in the *Retirement Savings Accounts Act 1997*; and
- (i) “transaction” means a rollover or transfer of an RSA holder’s benefits out of or into an RSA provider where the RSA holder gives their non written consent using the identifier given to that RSA holder by the RSA provider under item 2 of this Schedule.

This Determination replaces a previous Determination on this subject dated 30 June 1998.

Consent may be transmitted electronically, orally or in any other non written form, if, and only if, the procedure set out below is followed by the RSA provider in obtaining that consent.

- (1) Prior to an identifier, which meets the conditions set out under item 2, being used in a transaction, the RSA provider shall give the RSA holder a document, comprising binding conditions of use (the “conditions”), setting out the respective rights and obligations of the RSA provider and the RSA holder with respect to a transaction, including:
 - (a) that the RSA holder shall not be liable for any losses arising from:
 - (i) fraudulent or negligent conduct of the RSA provider’s employees or agents in relation to a transaction; and
 - (ii) the RSA provider’s system or equipment malfunctioning, including non-completion of transactions and unreasonable delays in carrying out the RSA holder’s valid instructions; and
 - (iii) any unauthorised transaction where the RSA holder has not contributed to such a loss; and
 - (iv) any unauthorised transaction occurring after the RSA holder has notified the RSA provider that the security of the RSA holder’s identifier has been breached; and
 - (b) subject to paragraph (c), how any other losses will be reasonably allocated between the RSA provider and the RSA holder, based on each party’s contribution to the loss; and
 - (c) except in the case of the RSA holder’s fraudulent conduct in relation to a transaction, placing a maximum limit on the RSA holder’s liability for the loss, which must in no circumstances exceed the total amount of the RSA holder’s benefits in the RSA; and
 - (d) describing any default arrangement that the RSA provider has in place.
- (2) The RSA provider shall allocate an identifier that is:
 - (a) unique to the RSA holder; and
 - (b) capable of being solely held by, and confidential to, the RSA holder; and
 - (c) capable of verification by the RSA provider against its records.

Sufficient non written consent

- (3)** A transaction can only be validly made:
 - (a) after the RSA holder has properly conveyed his or her non written consent using the identifier; and
 - (b) after the identifier has been verified against the RSA provider's records; and
 - (c) after the RSA holder has been informed, at the time of the transaction, of any default arrangement that may apply to the transaction; and
 - (d) if the transaction is accurately recorded by the RSA provider (whether by electronic means or otherwise) in a form capable of being readily accessed and understood at any time during the period which records are required to be kept by or under law. The RSA provider must take reasonable steps to protect the information it holds from misuse and loss and from unauthorised access, modification or disclosure.

- (4)** To avoid doubt, if the RSA provider alters any of the conditions after giving them to the RSA holder (including implementing a default arrangement for the first time, or changing an existing default arrangement) the RSA provider must notify the RSA holder as soon as is practicable (but need not allocate a replacement identifier to the RSA holder).

Sufficient non written consent

EXPLANATORY STATEMENT ACCOMPANYING DETERMINATION FOR THE PURPOSES OF SETTING OUT THE FORM OF NON WRITTEN CONSENT SUFFICIENT FOR ROLLING OVER OR TRANSFERRING BENEFITS

Regulation 4.30(b) of the *Retirement Savings Accounts Regulations* (the ‘RSA Regulations’) allows for consent other than written consent, the form of which is determined by the Australian Prudential Regulation Authority (APRA) as sufficient in the circumstances, for, respectively:

- the acceptance by a Retirement Savings Account (RSA) of a rollover or transfer of benefits from another RSA or from a regulated superannuation fund or Approved Deposit Fund (ADF); or
- the rollover or transfer of benefits from an RSA.

APRA has determined forms of non written consent in this Determination (which replaces a previous Determination on this subject dated 30 June 1998).

The usage of non written consent is optional. It is for the RSA provider to decide whether the circumstances of the RSA are such that providing for non written consent for rollovers or transfers is viable or desirable. If an RSA provider chooses to accept non written consent to such transactions the Determination **must** be complied with. If, however, the RSA provider decides not to use non written methods of consent, then there is no need to for the Determination to be followed.

The object of this Determination is to set out the factors which will ensure sufficiency of the non written consent. The requirements set out in this Determination are not intended to regulate forms of non written consent on a detailed level, but are designed to ensure that non written forms of consent meet functions usually met by written forms of consent.

Background

Generally, under the RSA Regulations, an RSA holder’s benefit in a Retirement Savings Account cannot be rolled over or transferred unless the RSA holder has given consent.

Ordinarily, under the RSA Regulations, the provider of an RSA cannot accept a transferred benefit unless consent has been given by the RSA holder, or the RSA provider reasonably believes it has been given.

Under the RSA Regulations, consent may be written or in any other form as determined. The Determination sets out the allowable form of the non written consent. It applies to, but is not limited to, consent transmitted electronically, oral consent, and other forms of non written consent such as PIN numbers using a telephone key pad.

It should be noted that, under Section 25 of the *Acts Interpretation Act 1901* any mode of representing or reproducing words, figures, drawings or symbols in a visible form is considered as writing. Therefore, the Determination does not cover consent given in this manner.

The Determination complements the *Income Tax Assessment Act (ITAA)* and Regulations, which aim to provide for electronic commerce and increased diversity of administration in the superannuation system.

Sufficient non written consent

The Determination

The Determination comes into force on 1 July 2002. It consists of four clauses that outline the elements with which non written consent to rollover or transfer of benefits must comply if that consent is to be regarded as sufficient. Key terms used in the Determination are also defined.

A form of consent to a rollover or transfer, which is not in writing, will only be regarded as sufficient if it meets the requirements set out in the Determination.

The Determination does not direct which types of technology or methods are preferred, but rather seeks to identify what is achieved by written consent, and then ensure that non written consent also performs these functions.

The Determination aims to achieve a balance between protecting RSA holders and allowing scope for technological advances to be incorporated into the superannuation system.

Clause 1 - Liability and Disclosure Arrangements

Due to the lack of traditional forms of identification (ie. written signatures) able to be used for verifying non written consent, the Determination imposes a requirement that an identifier must be issued by the RSA provider to the RSA holder and used in all non written transactions. Whenever an identifier is issued, RSA holders have a responsibility to act reasonably in safeguarding the identifier. Generally, there should be differing levels of RSA holder liability and/or RSA provider liability established depending on the degree of culpability or negligence involved in unauthorised use of the identifier or improper transactions, in accordance with the Determination where applicable.

Clause One provides that before an RSA provider allocates an identifier to an RSA holder to be used in non written consent transactions ('transactions'), legally enforceable conditions of use must be given by the RSA provider to the RSA holder setting out the rights and obligations with respect to transactions.

Clause One also sets out requirements relating to liability. Within these parameters the RSA provider can formulate conditions of use that are suitable to the RSA provider's circumstances.

The following issues must be addressed in the conditions of use:

(a) that the RSA holder shall not be liable for any losses arising from:

As a means of providing protection for RSA holders, the Determination provides that in some circumstances RSA holders will not be liable for losses. Basically, the RSA holder will not be liable for loss which results from a transaction for which the RSA holder is not responsible, and to which the RSA holder has not contributed.

(i) fraudulent or negligent conduct of the RSA provider's employees or agents in relation to a transaction; and

Where a loss has occurred due to the fraud or negligence of the RSA provider's employees or agents, it would not be conscionable that the RSA holder be held liable, as they bear no responsibility for such losses.

Sufficient non written consent

(ii) the RSA provider's system or equipment malfunctioning, including non-completion of transaction and unreasonable delays in carrying out the RSA holder's valid instructions; and

The RSA provider is responsible for loss caused by the failure of the RSA provider's system or equipment. Such system or equipment malfunction may result in, for example, non-completion of a transaction or unreasonable delays in carrying out the RSA holder's valid instructions. If losses result from these circumstances, the RSA holder should not be liable as they are not responsible for causing the loss.

As the Determination aims to achieve media neutrality, an 'unreasonable delay' is best understood as being equivalent to a delay which would be considered unreasonable in a written consent environment.

(iii) any unauthorised transaction where the RSA holder has not contributed to such a loss; and

Where an RSA holder has not contributed to a loss which results from an unauthorised transaction, they should not be liable for any part of that loss.

(iv) any unauthorised transaction occurring after the RSA holder has notified the RSA provider that the security of the RSA holder's identifier has been breached; and

At the point in time where an RSA holder notifies the RSA provider that the security of their identifier has been breached, the RSA provider should immediately take steps to ensure that the identifier is no longer able to be used. The appropriate method to notify the RSA provider of a breach, such as calling the customer service telephone number, may be included in the conditions of use. The RSA holder should not be responsible for losses which occur after this time, as the RSA provider bears responsibility for ensuring that the compromised identifier is not accepted as a means of verification. If an identifier which has been reported as compromised is accepted at a later stage to authorise a non written transaction, the RSA provider is liable for any losses which occur.

(b) subject to paragraph (c), how any losses will be reasonably allocated between the RSA provider and the RSA, based on each party's contribution to the loss; and

As mentioned above, it is important that the liability for loss set out in the conditions of use be based on a fair allocation of responsibility. This is best achieved by ensuring that liability is allocated based on each party's contribution to the loss.

An RSA holder may be considered to have contributed to a loss where, for example, they have voluntarily disclosed their identifier; kept a record of the identifier (without making any reasonable attempt to disguise the identifier) in a place which is easily accessed by others in a manner which allows its purpose to be identified; or by committing other negligent acts which allow another person to access the RSA holder's account via a non written transaction.

When an RSA holder, through negligence, contributes to a loss they should, subject to the maximum liability limit provided for in (c), be liable for such a loss.

Sufficient non written consent

(c) except in the case of the RSA holder's fraudulent conduct in relation to a transaction, placing a maximum limit on the RSA holder's liability for the loss, which must in no circumstances exceed the total amount of the RSA holder's benefits in the RSA; and

It is appropriate that the liability of the RSA holder differs according to the degree of culpability involved in the action which leads to the loss. It is reasonable that the RSA holder, except in cases of fraud, should not be liable for an amount which exceeds their total benefits in the RSA. For example, an RSA holder may act negligently in not safeguarding their identifier so that an unauthorised transaction occurs. However, if in carrying out the transaction the RSA provider releases an amount which exceeds the benefits held by the RSA holder, then the RSA provider should be liable for the amount of the loss which exceeds the RSA holder's benefits. Only in cases of fraud in which the RSA holder is involved is the RSA holder potentially liable for an amount in excess of their benefit.

(d) describing any default arrangement that the RSA provider has in place.

Due to the complexity of rollover and transfer transactions, situations may occur where instructions are not clear or cannot be carried out. In a case where insufficient instructions are received, the RSA provider is permitted to use a default arrangement, provided that the RSA holder is made aware of the arrangement, and its implications, through the conditions of use. Details of the default arrangement must also be advised to the RSA holder at the time of the non written transaction.

A default arrangement, in cases where insufficient or unclear instructions have been received from the RSA holder to enable the RSA provider to make the transaction, may consist of not progressing the transaction until the RSA provider has made contact with the RSA holder and received further information which is sufficient to complete the rollover or transfer.

The need to use the default arrangement may be ameliorated by seeking the necessary information in a structured manner eg. a stepped system where the instruction cannot be finalised until all steps are completed and all information is received and confirmed.

It should be noted that Regulation 99E of the ITAA, inserted by Statutory Rule No 14 effective 1 July 1998, provides that instructions must include information sufficient:

- to identify the amount and destination of any rollover payment; and
- to identify the amount of any cash amount; and
- to identify the tax components and preservation amounts of each rollover payment and cash amount; and
- to indicate how any 15 February 1990 rollover balance (if known) is to be distributed.

Clause 2 - Allocation of an Identifier

The identifier fulfils the functions of a written signature, including identifying the signer and allowing the signer to take a positive act to express approval and/or authorisation of the non written message. Any model of identifier and related delivery technology is acceptable provided it meets the requirements set out in the Determination.

A Tax File Number must not be used as an identifier.

Sufficient non written consent

Clause 2 provides that if the RSA provider proposes to accept non written forms of consent, the RSA provider must allocate to the RSA holder an identifier which is:

(a) unique to the RSA holder; and

Written signatures are regarded as legitimating transactions due to the fact that they are able, ideally, to uniquely identify the person who signs. In order for the allocated identifier to fulfil that function it must, be recognisable as unique to the individual RSA holder. Examples of a unique identifier are a PIN number, password etc.

(b) capable of being solely controlled by, and confidential to, the RSA holder; and

The identifier, to be capable of being relied upon as a safe and secure means of authenticating a transaction, must remain under the sole control of the RSA holder it is issued to. The RSA provider must take steps to ensure that the RSA holder is aware of the need and obligation to keep the identifier safe and confidential.

The liabilities under Clause 1 of the Determination also reflect the fundamental importance of ensuring the identifier's confidentiality.

(c) capable of verification by the RSA provider against its records.

For an identifier to fulfil the purpose of safeguarding an RSA holder's benefits and authenticating a transaction, it must be able to be verified. If an identifier is not able to be checked against an RSA provider's records and its authenticity thereby confirmed, it does not have value.

Clause 3 - Non written Consent Transactions - Necessary Elements

A non written transaction authorising a rollover or transfer of benefits is only able to be validly made on satisfaction of the following requirements:

(a) after the RSA holder has properly conveyed his or her non written consent using the identifier; and

As set out above, in a non written environment the use of an identifier that is unique, confidential and able to be authenticated is the primary means by which the legitimacy of a transaction can be assured. The identifier must be used for an instruction to be considered valid.

(b) after the identifier has been verified against the RSA provider's records; and

To ensure the legitimacy of the consent the identifier must be confirmed as that of the RSA holder before a valid transaction can be made. This is comparable to confirming an RSA holder's signature prior to acting on their instructions in a written environment.

(c) after the RSA holder has been informed, at the time of the transaction, of any default arrangement that may apply to the transaction; and

As provided for in Clause (1)(d), it may be necessary, due to the potential complexity of rollover and transfer transactions, to utilise a default arrangement where the instructions received from the RSA holder are insufficient for the RSA provider to carry them out.

Sufficient non written consent

The existence and operation of a proposed default arrangement must be disclosed to the RSA holder in the conditions of use, issued under Clause 1.

If any default arrangement applies, it must also be advised to the RSA holder at the time the RSA holder issues non written instructions. This reminder ensures that the RSA holder is aware of the default arrangement, and implications thereof, at the time of issuing the transaction instructions.

(d) if the transaction is accurately recorded by the RSA provider (whether by electronic means or otherwise) in a form capable of being readily accessed and understood at any time during the period which records are required to be kept by or under law.

When non written forms of consent are used, it is essential that adequate records of transactions are retained which are able to be accessed and reproduced in an understandable form. Such records should be held for a sufficient period of time to satisfy any legal requirements applicable to an RSA's record keeping. If an RSA provider feels that it is appropriate that records are maintained beyond this time, it is, of course, open for them to do so. The RSA provider must take reasonable steps to protect the information it holds from misuse and loss and from unauthorised access, modification or disclosure.

As no form of record maintenance is prescribed, storage in electronic forms using decoding, compression, conversion of data, or by other means is permitted.

Clause 4 - To avoid doubt, if the RSA provider alters any of the conditions after giving them to the RSA holder (including implementing a default arrangement for the first time, or changing an existing default arrangement) the RSA provider must notify the RSA holder as soon as is practicable (but need not allocate a replacement identifier to the RSA holder).

The conditions of use, which, under Clause 1, the RSA provider must give to the RSA holder prior to the allocation of an identifier, sets out the respective rights and obligations of the RSA provider and the RSA holder with respect to a non written transaction.

Where the RSA provider alters the conditions of use, the change must be notified to RSA holders as soon as is practicable. Such changes may include alterations to the default arrangement, or implementation of a default arrangement where none previously existed.

It is important that the RSA holder is notified of any change to the conditions of use as soon as is practicable as the change may impact on the RSA holder's decision to utilise non written arrangements.

Any change to the conditions of use does not, however, void the original conditions, and it is not necessary for the RSA holder to be allocated a new identifier.

Dated 31 January 2002

(Published by authority of the Australian Prudential Regulation Authority)