Australian Banking Association

ABA response to ePayments Code further policy consultation

ABA thanks ASIC for granting additional time to respond to the latest policy consultation on the ePayments Code review. ABA would be pleased to discuss the issues raised in this response, noting these include proposals for amendments to the ePayments Code as well as issues for joint discussion with ASIC and AFCA about the application of the Code.

Mistaken internet payments (MIP)

Proposal C1(a), Attachment B

If ASIC intends to incorporate the information from Attachment B as a Note in the ePayments Code, it may be useful to simplify the factors. If ASIC intends to provide the information as guidance, then ABA proposes the following changes to Attachment B.

- Return of all or some of the funds would be inconsistent with any other Commonwealth, State or Territory laws *or regulatory obligations*.
- Return of all or some of the funds would result in an overdrawing of the unintended recipient's account *where that was not the case before the mistaken internet payment*.
- *The receiving bank has knowledge of information indicating that* return of all or some of the funds would put the unintended recipient into a position of financial hardship that they weren't in before the mistaken internet payment.
- *If the unintended recipient is entitled to be consulted,* The unintended recipient reasonably believed they were entitled to the funds.

ABA asks ASIC to consider providing more specific guidance and/or work with AFCA to provide additional certainty. Processing partial refunds will require subscribers to apply more discretion. This creates the risk of banks adopting differing approaches based on internal policies and procedures. This can be a detrimental experience for customers and be an additional source of frustration. ABA asks ASIC to consider more specific guidance including:

- what is the minimum partial amount?
- how many attempts to make (it would not be reasonable to expect a receiving ADI to make daily attempts)
- how long should a receiving ADI generally attempt to retrieve funds – four weeks may be a reasonable period
- whether ASIC's guidance is in addition to, or intended to replace, AFCA's current expectations of the receiving bank. These include the receiving bank:
  - preventing the unintended recipient from withdrawing funds from their account (for example, freezing the money that remains in the account at the time or switching the account to deposit only);
  - writing to the unintended recipient and advising them it will withdraw funds from their account, if the unintended recipient does not establish that they are entitled to the funds.

In addition, ABA understands ASIC is open to considering including examples in the guidance. ABA provides the following examples for ASIC's consideration.

- If an unintended recipient has partial funds in the account but transaction history indicates the customer will have more funds coming with the next fortnightly or monthly pay cycle: Receiving ADI may decide to process a partial refund immediately and process a further refund after the next pay cycle.

- If an unintended recipient has limited funds in the account, and receiving ADI does not know when more funds will be coming into the account: Receiving ADI can process a partial refund immediately; after 4 weeks, no further funds have come into the account. The receiving ADI may decide to close the matter, even if it means not giving a full refund.
    - It would be helpful to clarify that a receiving ADI is not expected to check the recipient's account daily. Also, a receiving ADI can only make an educated guess about when funds may be paid into the account. If the unintended recipient receives funds into the account but the fund is withdrawn before the receiving ADI checks the account, the receiving ADI should not be liable for refunding the amount.
    - ABA understands consumer groups provided a case study where a receiving ADI provided a refund after a year. This is likely to be an unusual case. While the ePayments Code should not *prevent* a receiving ADI seeking to return funds after a longer period, guidance can clarify that attempting to retrieve funds for 4 weeks would usually constitute the making of reasonable endeavours.
- If an unintended recipient has limited funds in the account, and the dollar amount of the MIP is large, the bank may seek the unintended recipient's consent to entering a payment plan. This would include consent to the return of funds and the amount of repayments.

Proposal C2(a)

ABA supports the proposal that a sending ADI should be required to send a MIP request as soon as practicable and in any case no later than 5 business days.

ABA highlights this appears to be inconsistent with AFCA's current view that a MIP request should be raised by the sending ADI within two business days and any longer is unreasonable. ABA seeks joint discussions with ASIC and AFCA to ensure the ePayments Code is applied as intended.

Proposal C2(b)

ABA provides the following comments on record keeping about MIP requests. ABA notes having clearer guidance about what constitutes reasonable endeavours would significantly assist industry to ensure relevant records are maintained to assist AFCA.

Sending ADI:

- Query if it is necessary to retain records of '*details* of what sending ADI took into account in its investigation'. Information relevant to an AFCA review should be covered by the item 'reasons for and date of sending ADI's view that the transaction was or was not a MIP'.

Receiving ADI

- Keeping records of the acknowledgement may not be required where an ADI currently act on the case the same day as the ADI issue acknowledgement to the sending ADI. There will be other records kept showing the date in which the case was actioned. Also query if necessary to retain the *content* of receiving ADI's acknowledgement of the request.
- 'Date on which receiving ADI checked the account of the unintended recipient and informed the sending ADI of whether there were sufficient funds in the account': we seek clarification whether this only requires the ADI to keep a record of the fact that it has checked the account and informed the sending ADI, or also keep records about funds available in the account?
- 'Details of what the receiving ADI took into account in reaching a view that there was not a MIP (if relevant)' seems to duplicate: 'Reasons for and date of the receiving ADI's view that the transaction was not a MIP'. We propose this record should only be required if the receiving ADI determines a request is not a MIP, and seek clarification whether ADIs can apply their existing record keeping processes to comply.

- ‘Broadly, the factors that led the receiving ADI to a decision as to whether to pursue the full amount or only a partial amount of the MIP’: query whether this record is only necessary if the receiving ADI intends to pursue a partial refund. We also seek clarification of the level of detail required, or whether ADIs can apply existing record keeping processes to comply. Further discussions may be merited with ASIC and AFCA on specific questions such as keeping records where the ADI has assessed a full refund can send a customer into hardship.
- ‘Details of the ‘reasonable endeavours’ undertaken to return the funds’: we seek clarification of the level of detail needed, or whether ADIs can apply existing record keeping processes and be taken to comply. Query why this information would be relevant for AFCA, if AFCA cannot take the receiving ADI’s conduct into account in deciding the liability of the sending ADI. If ASIC proceeds with the proposal, query if the receiving ADI needs to keep records of the account balance every time the ADI checks the account.

Proposal C2(d)

ABA agrees the sending ADI should not be liable for the customer’s loss if the receiving ADI has not complied with the Code.

This approach may raise questions about the sender’s avenues to seek compensation in those circumstances. ABA notes ASIC’s commentary that there may be scope to develop an industry approach to address this issue, and agrees there can be merit in a clearer framework around how the ADIs should deal with customer’s loss in such circumstances. If ASIC wishes to consider this point further, ABA would strongly encourage ASIC to engage further with industry to understand the context for any further work (including differences in payment scheme rules).

Proposal C4

ABA notes that an expectation for industry to test, learn and adapt their warnings should not become a quasi regulatory requirement to also *report* to ASIC about these endeavours on a regular basis.

Seeking clarity about redacted statements

AFCA sometimes requires redacted account statements of the recipient account, where the sending ADI has delayed in raising a MIP request and the receiving account statements would show AFCA whether the delay caused the customer’s loss from the MIP (i.e. whether all or some of the funds from the MIP were still in the account at the time the sending ADI should have raised a MIP request). ABA seeks clarity from ASIC and AFCA on the receiving ADI’s obligation to provide these statements to the sending bank to assist AFCA.

Unauthorised transactions

Proposals E1 and E2

If some remote access scams will remain in the ePayments Code as unauthorised transactions, industry seeks further clarity from ASIC and AFCA on which scenarios or cases will be taken to be ‘unauthorised’ and which will be ‘authorised’.

ABA understands that ASIC’s view may be that:

- Unless the customer has specifically authorised a payment (ie, by clicking the ‘confirm’ button), the customer is not taken to have authorised a payment. As such the payment is prima facie *unauthorised*.
- However, this then raises a question about whether the customer has breached any passcode security requirements or otherwise have *contributed* to the loss.

ABA seeks clarification from both ASIC and AFCA about this interpretation and its application to a range of scenarios. For example:

- A customer downloads remote access software (note this requires a customer to acknowledge system permissions and terms of service when downloading the app), then logs onto their online banking browser or app. The scammer creates transactions. From the bank's visibility, the transaction was done on the customer's own computer or device, as such to bank systems it appears as though the customer inputted the transaction. ABA understands this is not an issue on Apple phones - remote access on Apple phones only allows view only so any transactions on these devices must have been entered by the customer.
- A customer gives their credentials knowingly to scammers purporting to be representatives from legitimate companies, for example to pay for postage, a small transaction, a modem. The customer may provide access to the customer's login credentials and passwords, or the customer stores these credentials on their computer or mobile device so these can be accessed by the scammer. The customer allows the scammer to access their internet banking through remote access. The scammer can then access the customer's details through keylogging software. This example is akin to the customer giving their debit card pass code to another person.

Linked transactions: specifically, ABA seeks discussions jointly with ASIC and AFCA about the treatment of 'linked' transactions. In these transactions, the customer takes action that results in the scammer obtaining access to the customer's online banking. The scammer makes a *first* transfer from one account held by the customer to a linked account. The customer then makes a *second* transfer out of the linked account to an account controlled by the scammer. ABA understands:

- ASIC staff's view is that the two transactions should be assessed separately. In the first transaction, the payment was *unauthorised* as it was made by the scammer, but the customer did not suffered loss from the transaction. In the second transaction, the payment was *authorised* as it was made by the customer.
- AFCA applies a different, 'but for' test to these transactions. AFCA would say that 'but for' the original unauthorised transfer between the customer's accounts, the loss from the subsequent authorised transfer would not have been incurred and would award compensation for this.

It is critical for industry and customers to have clarity and certainty about the application of the ePayments Code to this type of transaction and other scenarios. ABA requests follow up discussions with ASIC and AFCA on this aspect of the matter in 2021 or early 2022.

Specific clause dealing with remote access

ABA has previously asked ASIC to consider a specific rule dealing with remote access and customer's liability in cases where the bank can prove, on the balance of probabilities:

- Remote access allowed the other person to gain access to passcodes; or
- Remote access allowed the other person to gain access to the customer's online banking (app or in-browser);

and this contributed to loss.

Clarifying the concept of contribution to loss

As a fallback, ABA has had further discussions with ASIC staff that clause 11.3 should be amended to clarify that if a customer's action granted remote access to their computer or mobile device, this action is a relevant factor in assessing whether the customer contributed more than 50% to the loss.

Noting that the ePayments Code cannot deal in specifics, ABA asks ASIC to take into account the following scenarios when considering amendments to clause 11.3:

- A customer downloads remote access software (note this requires a customer to acknowledge system permissions and terms of service when downloading the app), then

logs onto their online banking browser or app. The scammer creates transactions within the app or browser using remote access software. From the bank's visibility, the transaction was done on the customer's own computer or device, as such to bank systems it appears as though the customer inputted the transaction.

- A customer downloads remote access software as described above. A transaction is created in online banking, which requires a One Time Pin (OTP) to authorise. A bank's system records that an OTP was issued to the customer's phone and the OTP was used to authorise payment. There is no evidence that the customer's phone number was ported without their knowledge. On some mobile devices, a customer needs to open a text message to view the OTP; but on other devices, the OTP is visible from the push notification when an SMS is received. Some phones will ask the customer whether they wish to copy the OTP, thus making the OTP visible.

Meaning of disclosure: In addition, ABA seeks further joint consideration by ASIC and AFCA on when remote access results in voluntary disclosure of a passcode. Even if ASIC does not propose to define 'voluntary disclosure', industry and customers would all benefit from a consistent approach to this issue. The approach should recognise that, once a customer has granted remote access to their computer or mobile device, a scammer can use software to see a passcode even if it appears as dots or asterisks on screen. Discussions can consider the relevance of banks issuing a clear, proximate warning about not disclosing a pass code, similar to the proposed approach to a warning in proposal C4.

Meaning of 'loss' in clause 10.3

ABA seeks clarification about the interpretation of clause 10.3.

Clause 10.3 is largely open ended and is a challenge to interpret in a scenario where the subscriber is managing an unauthorised transaction. The definition of 'loss' can be interpreted extremely broadly. It seems the intent of the clause it to ensure the customer is not liable for any loss arising from the transaction being disputed. For example, if there is an international transaction which was unauthorised then the expectation is that the customer is refunded the transaction value and the associated FX fee.

The extreme end of the interpretation is that the customer is refunded any bank fees and credit or debit interest for the period in which the funds.

Modernising the Code

Proposal F1

ABA has discussed with ASIC our concerns about the proposal to add references to 'authentication methods', without also updating clause 12 or otherwise adding biometric security standards.

Biometrics are not currently regulated by the ePayments Code, which gives subscribers some flexibility to consider a range of circumstances and market developments. Bringing biometrics into the Code also imposes the Code's liability regime to payments made using a biometric, specifically, clauses 10 and 11 will provide that a user is not liable for loss in some circumstances where an authentication method – such as a biometric – is used to make a payment. Without adjusting the liability regime to account for differences between a pass code and a biometric, the liability regime will not be fit for purpose:

- Clause 10.1 provides, for example, an unauthorised transaction performed after the subscriber has been informed that security of a pass code has been breached. This provision reflects the subscriber's role in issuing a replacement pass code. However, a subscriber cannot cancel, suspend or re-issue a biometric. This action needs to be taken by the holder. As such query whether a subscriber should still be held liable for a loss if a holder fails to take the necessary action, such as to delete biometics registered on their mobile device and re-registering the holder's biometrics.
- Clause 11 refers to the holder being liable for loss if the holder breaches the passcode security requirements. ASIC proposes to amend clause 11, without updating clause 12 or

otherwise adding biometric security requirements. This means the holder will not be liable for loss, even where the loss results from the holder's action – for example, by allowing another person to register a fingerprint on the holder's mobile device. Biometric authentication can be used on its own to authorise payments and is therefore, another form of passcodes. ASIC's approach can significantly increase of subscriber liability for losses in circumstances where the holder, not subscriber, needs to take action to remedy the breach. ABA's proposed biometric security requirements align with advice for consumers about protecting their mobile devices, including from government. ABA understands some banks address this issue in their disclosures or terms and conditions.

If ASIC proceeds with this proposal, ABA strongly advocates that ASIC also:

- Reviews clause 12 or otherwise amend the ePayments Code to provide that a holder is liable for a loss where the holder breaches the following requirements:
  - A user must not allow anyone else to add their biometric as an authentication method;
  - where a payment can be authorised by unlocking an electronic device (and no further authentication is needed to access online banking), a user must not allow anyone to access the electronic device when it is unlocked;
  - where a payment can be authorised by authenticating and accessing online banking, a user must not allow anyone to access the electronic device when the user has authenticated or has access to online banking;
  - where a holder identifies a breach of biometric security, the holder has responsibility for taking action to mitigate the breach, such as by deleting the biometrics registered to the mobile device and re-register the holder's biometrics.
- Review clause 9.1 or otherwise review the ePayments Code to provide that, where a biometric is used to authorise a payment (for example, using a fingerprint to authorise a specific payment), the transaction is taken to be an *authorised* payment.

ABA has provided a more detailed review of this proposal in Attachment A.

Proposal G1

ABA asks ASIC to consider whether all subscribers should be members of an external dispute resolution scheme, noting this requirement can be drafted to facilitate subscribers joining EDR schemes other than AFCA as the payments ecosystem continues to evolve.

New proposal: updating clause 7 for digital products

ABA provides a new proposal for amendments to clause 7, to accommodate or reflect how transaction history and other information are given to users in digital products such as digital wallets.

ABA notes these proposals are consistent with, but can also be seen as going beyond, the scope of clause 21 in facilitating electronic communications. ABA would be happy to discuss the reasoning for these proposals in more detail.

Clause 7.1: the current drafting reflects an expectation that subscribers provide a printed statement to their customers on a periodic basis, which includes all transactions undertaken during that period.

For some digital products, this is increasingly inconsistent with the way that customers expect to have access to their transaction history. Instead of a hard copy, printed statement, customers expect to have access to recent transactions in digital form (such as in-app). Customer may also expect to see information specific to a transaction, such as repayment history.

ABA proposes clause 7.1 be amended to specify that a 'statement' may be a statement accounting of a transaction, and such a statement may be provided on a transaction by transaction basis to reflect the facility through which the transaction is made.

Clause 7.4: the drafting in clause 7.4 also reflects an expectation that subscribers provide a hard copy, printed statement to customers on a periodic basis, and the paper statement would include the prescribed information.

Specifically for information prescribed in clause 7.4(f) and (g), this is increasingly inconsistent with how customers are able to query and dispute transactions in a digital environment. For example, rather than including 'contact information' for querying or disputing a transaction – which implies a phone number – a customer may use in-app features to seek further information about and/or to dispute a transaction.

ABA proposes clause 7.4 be amended to reflect that a 'statement' may be a statement accounting for a single transaction, and that the information prescribed under clause 7.4(f) and (g) may be located in the vicinity of the statement accessible electronically with the facility through which the transaction is made.

Privacy guidelines

ABA asks ASIC to consider whether this is the right time to introduce a detailed privacy guideline in clause 22, since the Privacy Act is currently under review.

Specifically, ABA asks ASIC to review the following aspects of the proposed privacy guidelines:

- Dot point 3: ABA asks ASIC to ensure the drafting is fully consistent with the relevant provisions of the Privacy Act. Small inconsistencies in drafting can raise questions about whether ASIC is intending to introduce a different requirement, thus creating uncertainty.
- Dot point 7: ABA seeks clarity about the disclosures that subscribers are expected to provide, and which requirements are contemplated in the reference to 'requirements that subscribers must meet when collecting personal information under APP 3'. The only requirement under APP 3 is that personal information is reasonably necessary for, or directly related to, one of the entity's functions and activities. ABA proposes that ASIC could refer to the OAIC's guidance on this APP, rather than creating new guidance that may result in further uncertainty.
- Dot point 9: provides that 'Clause 21 of the Code could specify that subscribers should provide users with a convenient process for users to update their contact details regardless of whether they provide users with information electronically or otherwise, in accordance with APP 12'. This is not a specific requirement of APP 12. APP 12 requires that an entity provide access to an individual's personal information on request, with certain exceptions. If ASIC proceeds to introduce this guidance, ABA asks for confirmation that online banking would meet these requirements.

Australian Banking Association

Attachment A – authentication methods

This table is provided to facilitate ASIC's review of the ePayments Code. The table sets out:

- how ASIC proposes to include references to 'authentication method' in the ePayments Code (with new references to authentication method in red).
- ABA's comments and proposals in blue.

Current ePayments Code	**Proposed amendments to include authentication method**
2.6 Existing definitions of 'device' and 'passcode'	The use of an individual's physical/biological characteristics to verify their identity.
4.6 Subscriber having to give information: - Fees and charges for replacing passcode - Description of how to report loss, theft or misuse of passcode (& must have process to allow reporting)	
4.9 disclosure requirement does not apply to low value facility	
4.11 Subscriber must give notice for increase in fees for replacing passcode (20 days)	
8.1 Mandatory consumer warning: If passcode is required to perform transactions, and subscriber provides monthly statement, the statement must at least annually provide a prominent, self contained explanation of PSRs	
9: Chapter C (liability does not apply to low value facilities.	
10.1 Holder not liable for loss: A holder is not liable for loss arising from an unauthorised transaction if the cause of the loss is: - pass code which is forged, faulty, expired or cancelled - a transaction requiring a pass code that occurred before the user received the pass code (including a reissued pass code) - an unauthorised transaction performed after the subscriber has been informed that security of a pass code has been breached	Holder not liable for loss: A holder is not liable for loss arising from an unauthorised transaction if the cause of the loss is: - a transaction requiring other authentication method in place of a pass code that occurred before the user received and/or registered for use of the other authentication method (including re-registration of another authentication method) ABA seeks clarification if this refers to a transaction authorised by biometric occurring before a biometric is registered? - an unauthorised transaction performed after the subscriber has been informed that security of an authentication method has been breached.

For a biometric, the holder (or another person) can take action to delete / change a biometric, this matter is not within subscriber's control. As such query if subscriber should be liable in this scenario.

Further, ABA notes ASIC is seeking stakeholder feedback on whether there should be a new definition of 'authentication method security' (to distinguish it from the pass code security requirements) and, if so, how it should be defined.

ABA proposes ASIC should define 'authentication method security' and include requirements relating to biometrics.

- Refer proposed security requirements for biometrics in clause 12, including a user must not allow another person to register their biometric on the mobile device.
- In addition, when a holder identifies and informs a subscriber that the biometric authentication method is breached, the holder should take reasonable steps to re-secure it, such as deregistering all biometrics from the mobile device and re-registering the holder's.

10.2 When holder not liable for loss:

A holder is not liable for loss arising from an unauthorised transaction that can be made using an identifier without a pass code or device.

Where a transaction can be made using a device, or a device and an identifier, but does not require a pass code, the holder is liable only if the user unreasonably delays reporting the loss or theft of the device.

When holder not liable for loss:

A holder is not liable for loss arising from an unauthorised transaction that can be made using an identifier without an authentication method.

ABA seeks clarification what circumstances this would apply to.

Where a transaction can be made using a device, or a device and an identifier, but does not require an authentication method, the holder is liable only if the user unreasonably delays reporting the loss or theft of the device.

ABA proposes this provision recognise that, if a holder is required to use a biometric to open the banking app, and then transactions / payments do not require re-authentication, the holder should be liable for that payment.

10.4 When holder is not liable for loss:

In dispute about whether user received a pass code:

- presumption that user did not received it unless subscriber can prove they did
- can prove receipt by getting an acknowledgement of receipt from user

- cannot rely on proof of deliver to address

10.5 When holder Is not liable for loss:

Cannot have any terms and conditions that deem a pass code sent to the correct address to be received by user

11.2 When holder is liable for loss:

Where a subscriber can prove on the balance of probability that a user contributed to a loss through fraud, or breaching the PSRs:

- holder liable for full loss before fraud/breach of PSRs is reported to subscriber
- holder not liable for loss that exceeds transaction limits, on any facility where the holder and subscriber had not agreed could be accessed using the device, identifier and/or pass code used to perform the transaction.

If ASIC amends the ePayments Code to include standards for biometric security, this provision should also apply to determine when a holder is liable because of a breached biometric.

11.3 Where holder is liable for loss:

Where:

(a) more than one pass code is required to perform a transaction, and

(b) a subscriber proves that a user breached the PSRs for one or more of the required pass codes, but not all of the required pass codes,

the holder is liable only if the subscriber also proves on the balance of probability that the breach of the PSRs was more than 50% responsible for the losses, when assessed together with all the contributing causes.

Where holder is liable for loss:

Where:

(a) more than one authentication method is required to perform a transaction, and

(b) a subscriber proves that a user breached the PSRs for one or more of the required authentication methods, but not all of the required authentication methods,

the holder is liable only if the subscriber also proves on the balance of probability that the breach of the PSRs was more than 50% responsible for the losses, when assessed together with all the contributing causes.

If PSRs only apply to pass codes and not biometrics, this provision should not refer to authentication methods.

If clause 11.3 is amended and ASIC also includes the proposed biometric security standards, there will still be questions about how a subscriber could prove that a biometric security breach was more than 50% responsible for a loss. Joint work with ASIC and AFCA may help to mitigate uncertainty and inconsistent outcomes.

11.5 When holder is liable for loss:

Where a subscriber can prove, on the balance of probability, that a user contributed to losses resulting from an unauthorised transaction by unreasonably delaying reporting the misuse, loss

When holder is liable for loss:

Where a subscriber can prove, on the balance of probability, that a user contributed to losses resulting from an unauthorised transaction by unreasonably delaying reporting the misuse, loss or theft of a device, or that the security of all

or theft of a device, or that the security of all pass codes has been breached, the holder:	authentication methods has been breached, the holder:
(a) is liable for the actual losses that occur between when the user became aware of the security compromise, or should reasonably have become aware in the case of a lost or stolen device, and when the security compromise was reported to the subscriber, but	(a) is liable for the actual losses that occur between when the user became aware of the security compromise, or should reasonably have become aware in the case of a lost or stolen device, and when the security compromise was reported to the subscriber, but
(b) is not liable for any portion of the loss that exceeds transaction limits, on any facility where the holder and subscriber had not agreed could be accessed using the device, identifier and/or pass code used to perform the transaction	(b) is not liable for any portion of the loss that exceeds transaction limits, on any facility where the holder and subscriber had not agreed could be accessed using the device, identifier and/or authentication methods used to perform the transaction.
11.6 (effect of charges) In deciding whether a user has unreasonably delayed reporting the misuse, loss or theft of a device, or a breach of pass code security, the effect of any charges imposed by the subscriber for making the report or replacing a device or pass code must be taken into account.	In deciding whether a user has unreasonably delayed reporting the misuse, loss or theft of a device, or a breach of authentication method security, the effect of any charges imposed by the subscriber for making the report or replacing a device or authentication method must be taken into account. Query if this is applicable to deleting or changing a biometric.
11.7 Limited liability: Where a pass code was required to perform an unauthorised transaction, and clauses 11.2–11.6 do not apply, the holder is liable for the least of:	Limited liability: Where an authentication method was required to perform an unauthorised transaction, and clauses 11.2–11.6 do not apply, the holder is liable for the least of:
(a) $150, or a lower figure determined by the subscriber,	(a) $150, or a lower figure determined by the subscriber,
(b) the balance of the facility or facilities which the subscriber and the holder have agreed can be accessed using the device and/or pass code, including any prearranged credit, or	(b) the balance of the facility or facilities which the subscriber and the holder have agreed can be accessed using the device and/or authentication method, including any prearranged credit, or
(c) the actual loss at the time that the misuse, loss or theft of a device or breach of pass code security is reported to the subscriber, excluding that portion of the losses incurred on any one day which exceeds any relevant daily transaction or other periodic transaction limit.	(c) the actual loss at the time that the misuse, loss or theft of a device or breach of authentication method security is reported to the subscriber, excluding that portion of the losses incurred on any one day which exceeds any relevant daily transaction or other periodic transaction limit.
11.8 Proof that user contributed to loss In deciding whether a subscriber has proved on the balance of probability that a user has contributed to losses under clauses 11.2 and 11.5:	Proof that user contributed to loss In deciding whether a subscriber has proved on the balance of probability that a user has contributed to losses under clauses 11.2 and 11.5:
(b) the fact that a facility has been accessed with the correct device and/or pass code, while	(b) the fact that a facility has been accessed with the correct device and/or authentication method,

significant, does not, of itself, constitute proof on the balance of probability that a user contributed to losses through fraud or a breach of the pass code security requirements in clause 12	while significant, does not, of itself, constitute proof on the balance of probability that a user contributed to losses through fraud or a breach of the pass code security requirements in clause 12. If ASIC incorporate standards relating to biometric security in the Code, there should be a reference to these standards in this provision. Otherwise, query if this provision would be appropriate. For a payment to be made using a biometric, the holder would have had to access the mobile device/app themselves or allowed another person to register their biometric.
11.9 Discretion to reduce liability: Where a subscriber has not applied a reasonable daily or other periodic transaction limit, the subscriber, or an external dispute resolution body, may reduce the liability of the holder for an unauthorised transaction under clauses 11.2–11.7 by such amount as it considers fair and reasonable, taking into account: (c) if the unauthorised transaction involves accessing a credit facility, including drawing on loan repayments made to a loan facility that is accessible using a device and/or pass code, whether, at the time of making the credit facility available using the device and/or pass code, the subscriber had taken reasonable steps to warn the holder of the risk of the device and/or pass code being used to make unauthorised transactions on the credit facility	Discretion to reduce liability: Where a subscriber has not applied a reasonable daily or other periodic transaction limit, the subscriber, or an external dispute resolution body, may reduce the liability of the holder for an unauthorised transaction under clauses 11.2–11.7 by such amount as it considers fair and reasonable, taking into account: (c) if the unauthorised transaction involves accessing a credit facility, including drawing on loan repayments made to a loan facility that is accessible using a device and/or authentication method, whether, at the time of making the credit facility available using the device and/or authentication method, the subscriber had taken reasonable steps to warn the holder of the risk of the device and/or authentication method being used to make unauthorised transactions on the credit facility. This provision makes sense if the ePC makes provisions about liability for biometric security.
12 (PSR) 12.2 A user must not: (a) voluntarily disclose one or more pass codes to anyone, including a family member or friend, (b) where a device is also needed to perform a transaction, write or record pass code(s) on a device, or keep a record of the pass code(s) on anything: (i) carried with a device, or (ii) liable to loss or theft simultaneously with a device, unless the user makes a reasonable attempt to protect the security of the pass code, or	ABA proposes additional provisions about biometric security to specify a user must not: (a) allow anyone else to add their biometric as an authentication method, (b) where a payment can be authorised by unlocking an electronic device (and no further authentication is needed to access online banking), allow anyone to access the electronic device when it is unlocked, (c) where a payment can be authorised by authenticating and accessing online banking, allow anyone to access the electronic device when the user has authenticated/has access to online banking. The provision dealing with biometric security also needs to recognise that the holder needs to take

(c) where a device is not needed to perform a transaction, keep a written record of all pass codes required to perform transactions on one or more articles liable to be lost or stolen simultaneously, without making a reasonable attempt to protect the security of the pass code(s).

12 (PSR)

12.3 A reasonable attempt to protect the security of a pass code record includes making any reasonable attempt to disguise the pass code within the record, or prevent unauthorised access to the pass code record, including by:

(a) hiding or disguising the pass code record among other records,

(b) hiding or disguising the pass code record in a place where a pass code record would not be expected to be found,

(c) keeping a record of the pass code record in a securely locked container, or

(d) preventing unauthorised access to an electronically stored record of the pass code record.

This list is not exhaustive.

12 (PSR)

12.4 A user must not act with extreme carelessness in failing to protect the security of all pass codes where extreme carelessness means a degree of carelessness that greatly exceeds what would normally be considered careless behaviour.

Note 1: An example of extreme carelessness is storing a user name and pass code for internet banking in a diary, BlackBerry or computer that is not password protected under the heading 'Internet banking codes'.

12 (PSR)

12.5 On or after 1 April 2002, a user must not select a numeric pass code that represents their birth date, or an alphabetical pass code that is a recognisable part of their name, if a subscriber has:

(a) specifically instructed the user not to do so, and

(b) warned the user of the consequences of doing so.

12 (PSR)

action to mitigate a security breach for a biometric.

ABA has previously provided an example of extreme carelessness involving biometric authentication.

Query if the ePC should specify a subscriber can give instructions and warnings about biometric

12.6 A subscriber must give the specific instruction and warning in clause 12.5:

(a) at the time of selecting a pass code,

(b) in a way that is designed to focus the actual user's attention specifically on the instruction and the consequences of breaching it, and

(c) taking account of the actual user's capacity to understand the instruction and warning.

12 (PSR)

12.8 Where a subscriber expressly authorises particular conduct by a user, either generally or subject to conditions, a user who engages in the conduct, complying with any conditions, does not breach the pass code security requirements in clause 12.

12 (PSR)

12.9 Where a subscriber expressly or implicitly promotes, endorses or authorises the use of a service for accessing a facility (for example, by hosting an access service on the subscriber's electronic address), a user who discloses, records or stores a pass code that is required or recommended for the purpose of using the service does not breach the pass code security requirements in clause12.

Note 1: For example, if a subscriber permits users to give their pass code(s) to an account aggregator service offered by the subscriber or an associated company, a user who discloses their pass code(s) to the service does not breach the pass code security requirements in clause 12.

Note 2: For example, if a subscriber permits the storage of pass codes in an electronic folder in the user's computer, a user who stores their pass code(s) in this way does not breach the pass code security requirements in clause 12.

13: PSR guidelines

13.1A subscriber may give users guidelines on ensuring the security of devices and pass codes in their terms and conditions or other communications.

Note: Subscribers must provide a process for users to report the loss, theft or misuse of a device or pass code: see clause17. Subscribers must include on or with statements, at least annually, a summary of the pass code security guidelines under clause13: see clause 8.

security. The instructions and warnings may be general in nature and not specific to the user's specific electronic device.

If a warning is given, this should flow through to the allocation of liability.

ABA queries whether the ePC should allow a subscriber to give users guidelines on biometric security in T&Cs and other communications.

17.1 (reporting unauthorised transaction, loss and theft): A subscriber must have an effective and convenient process for users to report: (a) unauthorised transactions, (b) loss, theft or misuse of a device, or (c) breach of pass code security.	17.1 (reporting unauthorised transaction, loss and theft): A subscriber must have an effective and convenient process for users to report: (a) unauthorised transactions, (b) loss, theft or misuse of a device, or (c) breach of authentication method security.
17.3 (reporting unauthorised transaction, loss and theft): If a user reports the loss, theft or misuse of a device or breach of pass code security, the liability of the holder for unauthorised transactions is limited by Chapter C of this Code.	17.3 (reporting unauthorised transaction, loss and theft): If a user reports the loss, theft or misuse of a device or breach of authentication method security, the liability of the holder for unauthorised transactions is limited by Chapter C of this Code. ABA proposes this provision should not apply where the holder needs to take action to remedy a breach of an authentication method.
20.1 (book-up): If a subscriber and a merchant have a merchant agreement, the agreement must prohibit the merchant from holding a user's pass code as part of a book up arrangement.	
38.2 (complaints procedures): If a user complains about an unauthorised transaction, the subscriber must make reasonable efforts to obtain from the user the following information: (a) the type of facility, (b) where relevant, an identifier, (c) the type of device and/or pass code used to perform the transaction, (d) the name and address of the holder, (e) the name of other user(s), (f) whether a device used to perform the transaction was signed by the user, (g) whether a device was lost, stolen or misused or the security of a pass code was breached and if so: (i) the date and time of the loss, theft or misuse of the device, or breach of pass code security, (ii) the date and time the loss, theft or misuse of the device, or breach of pass code security, was reported to the subscriber, and	38.2 (complaints procedures): If a user complains about an unauthorised transaction, the subscriber must make reasonable efforts to obtain from the user the following information: If ASIC incorporates standards relating to biometric security in the Code, this clause should be updated to include questions around biometric authentication so that ADIs collect this information at the time customer disputes a transaction. (a) the type of facility, (b) where relevant, an identifier, (c) the type of device and/or authentication method used to perform the transaction, (d) the name and address of the holder, (e) the name of other user(s), (f) whether a device used to perform the transaction was signed by the user, (g) whether a device was lost, stolen or misused or the security of an authentication method was breached and if so:

(iii) the date, time and method of reporting the loss, theft or misuse of the device, or breach of pass code security, to the police,

(h) where one or more pass codes were required to perform transactions, whether the user recorded the pass code(s), and if so:

(i) how the user recorded the pass code(s),

(ii) where the user kept the record, and

(iii) whether the record was lost or stolen, and if so, the date and time of the loss or theft,

(i) where one or more pass codes were required to perform transactions, whether the user had disclosed the pass code(s) to anyone,

(j) details of where and how the loss, theft or misuse of a device, or breach of pass code security, occurred (for example, housebreaking, stolen wallet),

(k) details of the transaction to be investigated, including:

(i) a description,

(ii) the date and time,

(iii) the amount, and

(iv) the type and location of electronic equipment used,

(l) details of any surrounding circumstances,

(m) any steps taken by the user to ensure the security of any device or pass code(s) needed to perform transactions that the user considers relevant to the liability of the holder, and

(n) details of the last authorised transaction performed using the facility.

(i) the date and time of the loss, theft or misuse of the device, or breach of pass code security,

(ii) the date and time the loss, theft or misuse of the device, or breach of pass code security, was reported to the subscriber, and

(iii) the date, time and method of reporting the loss, theft or misuse of the device, or breach of pass code security, to the police,

(h) where one or more authentication methods were required to perform transactions, whether the user recorded the pass code(s), and if so:

(i) how the user recorded the pass code(s),

(ii) where the user kept the record, and

(iii) whether the record was lost or stolen, and if so, the date and time of the loss or theft,

(i) where one or more pass codes were required to perform transactions, whether the user had disclosed the pass code(s) to anyone,

(j) details of where and how the loss, theft or misuse of a device, or breach of authentication method security, occurred (for example, housebreaking, stolen wallet),

ABA agrees with this amendment if this provision refers to the proposed standards relating to biometric security. Otherwise this provision should continue to refer to pass codes.

(k) details of the transaction to be investigated, including:

(i) a description,

(ii) the date and time,

(iii) the amount, and

(iv) the type and location of electronic equipment used,

(l) details of any surrounding circumstances,

(m) any steps taken by the user to ensure the security of any device or authentication method(s) needed to perform transactions that the user considers relevant to the liability of the holder, and

This provision should remain as is, as a customer cannot take steps to ensure the security of their biometrics. Alternately this provision could refer to the proposed biometric security standards.

(n) details of the last authorised transaction performed using the facility.