ASIC
Australian Securities & Investments Commission

REGULATION IMPACT STATEMENT

ePayments Code

September 2011

About this Regulation Impact Statement

This Regulation Impact Statement (RIS) addresses ASIC's proposals for the revised ePayments Code (formerly known as the Electronic Funds Transfer Code of Conduct).

What this Regulation Impact Statement is about

1 This Regulation Impact Statement (RIS) addresses ASIC's proposals for a revised version of the ePayments Code (formerly known as the Electronic Funds Transfer Code of Conduct). In particular, it addresses the two most important changes to the Code—namely, the tailored requirements for low value facilities and the recovery procedures for mistaken internet payments.

2 In developing our final position, we have considered the regulatory and financial impact of our proposals. We aim to strike a balance between:

- maintaining, facilitating and improving the performance of the financial system and entities in it;
- promoting confident and informed participation by investors and consumers in the financial system; and
- administering the law effectively and with minimal procedural requirements.

3 This RIS sets out our assessment of the regulatory and financial impacts of our proposed policy and our achievement of this balance. It deals with:

- the likely compliance costs;
- the likely effect on competition; and
- other impacts, costs and benefits.

Contents

A Introduction

Background

4 The Electronic Funds Transfer Code of Conduct (Code) is a voluntary industry code of practice covering most consumer electronic payments.

5 The Code has existed since 1986. Initially, it was a set of recommended procedures endorsed by federal and state consumer affairs ministers. These procedures were amended and relaunched as the Code in 1989.

6 The Code has always been seen as, and continues to be, best practice in consumer protection in the funds transfer and payment services industry. By subscribing to the Code, firms can publicly demonstrate their commitment to high standards of consumer protection. Since its inception, federal and state governments have encouraged industry to adopt the Code and maintain a continuing interest in the Code being widely followed within industry.

7 The existing Code does not have a statement of objectives. At its core, however, it deals with the allocation of liability for unauthorised electronic transactions.

8 The proposed new Code, to be known as the 'ePayments Code', would include a statement of objectives to help consumers and subscribers to the Code understand the context and objectives of the Code. Among other things, the objectives of the Code include providing:

(a) a quality consumer protection regime for payment facilities;

(b) clear and fair rules for allocating liability for unauthorised transactions; and

(c) a flexible regime that accommodates providers of new payment facilities.

9 The existing Code has a two-part structure. Part A governs the relationship between account institutions and their clients. Part B applies to stored value products.

10 Currently, 170 entities subscribe to the Code.[1] Table 1 provides a sample of current subscribers to the Code.

[1] A list of subscribers to the Code is available at www.asic.gov.au/asic/asic.nsf/byheadline/List-of-EFT-Code-members-A-H?openDocument.

Table 1: A sample of current subscribers to the Code

- Almost all banks, building societies and credit unions that offer electronic banking facilities
- ABB Grain Ltd
- American Express International
- Baptist Investments and Finance Ltd
- B & E Limited
- Collins Securities Pty Ltd
- Columbus Capital Pty Limited
- First Data Resources Australia
- GE Capital Finance Australia
- Hunter Mutual Limited
- Landmark Operations Limited
- LinkLoan Services Pty Limited
- MECU Limited
- Members Equity Pty Ltd
- Money Switch Limited
- Pioneer Mortgage Services
- Prime Mortgage Group Ltd
- RESIMAC Limited
- Rural Finance Corporation of Victoria
- Technocash
- Territory Insurance Office

11 Being a voluntary code, not all providers of electronic payment facilities subscribe to the Code. Nevertheless, the Code provides a long-standing industry benchmark that subscribers have found useful in streamlining their internal and external practices (e.g. how to allocate liability in certain situations).

12 From a consumer's perspective, dealing with a subscriber gives an additional layer of confidence when transacting using electronic payment facilities. For this reason, we encourage consumers to check whether a firm is a subscriber when considering whether to use their services. Consumers cannot assume that the same protections and safeguards are available when dealing with a non-subscriber.

13 ASIC has been responsible for the Code since 1998. We monitor subscribers' compliance with the Code and publish annual reports highlighting non-compliance by subscribers. As the administrator of the Code, we are also required to periodically review it.

14 This RIS has been prepared for the most recent review of the Code, which has been completed in 2011. Before this review, the Code was last reviewed in 2001. Since then, there have been significant developments in the electronic payment industry and the regulatory landscape. New electronic payment products and product issuers have entered the market and changed the way consumers transact.

15 The Code needs to be updated to maintain its relevance to the current products and practices in the electronic payment market. Changes to be introduced in the revised Code will provide more flexibility to subscribers and reduce their compliance costs. For example, subscribers may use electronic communication in delivering the disclosures required by the Code.

Assessing the problem

16 There are a number of problems relating to the existing Code's structure and scope. The first problem, dealt with in Issue One, concerns the Code's lack of coverage due to not being drafted in a technology neutral manner. The second problem, dealt with in Issue Two, concerns the lack of a uniform process for dealing with mistaken internet payments.

17 Since the Code was last reviewed a decade ago, new electronic payment products have entered the market. Products such as internet banking and contactless and mobile payments are increasingly being used by consumers. Some of these products are offered by subscribers to the Code, while others are offered by non-subscribers.

18 Historically, most of the subscribers to the Code were banks, credit unions and building societies. As such, much of the Code (Part A) was designed with the operations of the banking industry in mind.

19 Part B of the existing Code provides a 'light-touch' regime for stored value products.[2] At the time it was drafted, it was intended to give the providers of stored value products (as new products at the time) some flexibility so as not to hinder product innovation, while maintaining a level of basic consumer protection for users of these products. Part B is essentially a 'cut down' version of the rules in Part A.

20 In practice, Part B has been underused, partly because many newer electronic payment products are not covered by the definition of 'stored value facility'. For example, some products rely on remote authorisation, which is not covered by the definitions of 'stored value transactions' and 'stored value facilities'.

21 While some of the newer payment products could be covered by Part A of the Code, most providers of newer electronic payment products have not subscribed to the Code.

22 The fact that the existing Code is not drafted in technology neutral language limits its application to a wider range of products.

23 The benefit of Code subscription has been widely accepted in the banking industry. Consumers can expect that transactions performed using products or services provided by their banking institution to benefit from the additional protection offered by the Code. There is a community expectation that banking institutions adopt the Code, putting the pressure on participants in the industry to sign up to the Code.

[2] 'Stored value' is defined in the Code as a representation of value intended to be used for making a payment, which may or may not be denominated by reference to a unit of currency. 'Stored value facility' means a facility that is designed to control the storage and release of the stored value for making a payment, intended to be in the possession and control of a user, and contains a value control record (cl 11.2).

24 The benefit of Code subscription is less well understood to newer entrants to the payment market, who do not traditionally see themselves as providers of banking services.

25 Ultimately, the need for consistent and consistent levels of consumer protection for broader range of payment products leads to the question of whether membership of the Code should be made mandatory for all businesses offering electronic payment products. Traditional banking organisations have expressed concern that they may be disadvantaged compared to new entrants in the payment services field.

26 The Code is a voluntary Code, and mandating membership is not within the scope of ASIC's current powers. This is a matter for the government to decide. ASIC, together with industry participants, external dispute resolution schemes and other government agencies will monitor the efficacy of the current voluntary Code arrangement. If necessary, we will recommend a law reform to the government.

27 The use of new technologies in electronic payment products introduces new issues to the market. Other issues, such as mistaken internet payments, are not new but are more relevant today because internet banking services are widely used by consumers. For some of these issues, self-regulation frameworks have not been able to offer effective solutions.

28 The size of the electronic payment market is significant. For example, there were more than 135 million direct credit transactions (which include internet banking) in January 2011, with around $477 million transacted.[3] Problems affecting a small fraction of this market would still equate to a large number and value of transactions and individual consumers affected. Improvements to the payment system could potentially save costs for financial institutions through better processes and fewer consumer disputes in the long run.

29 Market share held by non-subscribers to the Code is notably increasing. For example, payment providers such as PayPal play an important role in the consumer payment market. PayPal has more than 4 million active accounts in Australia, with around US$92 billion reported for its total value of transactions in 2010.[4]

30 Consumers of financial services and products in Australia benefit from a level of consumer protection provided by a number of regulatory instruments including the *Australian Securities and Investments Commission Act 2001* (ASIC Act).[5]

31 Protection may also be available through contractual agreements between a consumer and a payment provider as specified in the Terms and Conditions

[3] Reserve Bank of Australia, www.rba.gov.au/statistics/tables/index.html#payments_system.
[4] PayPal Media Release 'Fast Facts', https://www.paypal-media.com/au/about at 23 August 2011
[5] Subdivision D, ASIC Act 2001 (Cth).

for the payment product or service. The robustness of Terms and Conditions vary between product issuers. For example, one mobile payment service provider states in their Terms and Conditions that it will not be liable for an unauthorised transaction where a consumer fails to report it within 30 days or where a password has been used to authenticate the transaction.[6]

32 The Code provides an additional layer of consumer protection by setting out, among other things, liability allocation mechanisms for unauthorised transactions performed using products offered by Code subscribers.

33 Consumers of products that are not covered by the Code might be able to seek redress for unauthorised transactions through small claims courts / tribunals. However this is unlikely to provide effective redress for the average consumer if the amount in dispute is of low value as the cost of pursuing these avenues is generally more than the amount that could be recovered.

34 The overall market size held by newer payment providers that do not currently subscribe to the Code is difficult to determine. Traditional payment products are offered by conventional authorised deposit-taking institutions (ADIs) such as banks, credit unions and building societies. Today the payment market is more open, with participants from different sectors (e.g. retail, software development, public transportation) entering the electronic payment market.

35 Newer payment product providers that operate outside the prudentially-regulated space are not required to publish data on their payment products. This, together with the broad and diverse membership of the newer payment product market segment, makes it difficult to assess the size of this market relative to the more conventional payment market already covered by the Code.

36 Some information is available to help us assess the direction of the newer payment market. In 2010, the size of mobile payment market in Australia was valued at $155 million.[7] While the market size is relatively small compared to the more traditional payment products that are already covered by the Code,[8] newer payment product market is growing rapidly. One report predicts that the volume of mobile payments would reach US$86.1 billion worldwide in 2011.[9]

[6] mHITs, 'Terms and Conditions', www.mhits.com.au/mHITs%20Limited%20Product%20Disclosure%20Statement.pdf
[7] Nielsen, 'Mobile commerce market sizing and opportunity study Australia' (2011), commissioned by PayPal: PayPal Australia Media Library, 'Smartphone growth fuels mCommerce adoption – Australian retail goes mobile', http://www.paypal-education.com.au/media/news_24032011.html
[8] In 2010, the average amount transacted each month was: $12 billion for EFTPOS transactions; $19.6 billion for credit card transactions; and $12 billion for ATM withdrawals: Australian Payments Clearing Association, 'Cards transactions – value', http://www.apca.com.au/Public/apca01_live.nsf/WebPageDisplay/Stats_CardValue
[9] Patrick Stafford, 'Mobile payments to reach $86 billion in 2011' (2001) *Smart Company*, http://www.smartcompany.com.au/information-technology/20110725-mobile-payments-to-reach-86-billion-in-2011.html

37 If we took no action in relation to newer electronic payment products, a large number of transactions and consumers may be subjected to the risk of losses without effective recourse when things go amiss. As the use of newer payment products becomes more prevalent, it is important that mechanisms are available to support consumers' use of, and confidence in the products.

Objectives of government action

38 The Code plays an important role in regulating electronic payment services in Australia. It complements other regulatory requirements, while also providing significant additional consumer protections in areas such as liability allocation for unauthorised transactions.

39 As the administrator of the Code, ASIC has an interest in ensuring its relevance and effectiveness.

40 As discussed in paragraph 8, the new Code would include a statement of objectives. Among other things, the new Code aims to provide:

(a) a quality consumer protection regime for payment facilities;

(b) clear and fair rules for allocating liability for unauthorised transactions; and

(c) a flexible regime that accommodates providers of new payment facilities.

41 The new Code's objectives and the proposed actions in this RIS are consistent with our mandate under the *Australian Securities and Investments Commission Act 2001* (ASIC Act), which includes facilitating and improving the financial system, and promoting confident consumer participation in the financial system.

42 We aim to broaden subscription to the Code, particularly to include newer participants in the electronic payment market. Subscription by more industry operators would improve the extent of consumer protection for products offered in the market, and help create a more level playing field among participants in the market. Being voluntary, the Code needs to be sufficiently attractive to potential subscribers. We have looked at how to make the Code attractive to a wider group of potential subscribers.

43 We have indicated earlier that whether or not the Code should be made mandatory is a matter for the government to decide. We also acknowledge that before the government can consider whether to legislate or mandate Code subscription, the Code needs to be promoted more vigorously both to

consumers and industry participants. As such, we do not currently consider making the Code mandatory as an option to the issues in this RIS.[10]

44 The success of the Code is largely determined by industry cooperation. As a voluntary industry code, the consensus-based nature of the Code has called for extensive stakeholder consultation throughout the review, the revision and the implementation of the new Code.

45 Some of the proposed actions call for system changes by many subscribers to the Code, which would require time, resources and costs to implement. We have used the review process to consult with stakeholders about the necessity and appropriateness of each change.

[10] Australian Securities and Investments Commission, Report 218: *Electronic Funds Transfer Code of Conduct review: Feedback on CP 90 and final positions*, 12-13.

B Issue 1: Non-traditional and low value facilities

Assessing the problem

46 As stated earlier, the Code as it presently stands is not technology neutral. The two parts of the Code, both parts A and B, were drafted with particular products and transactions in mind.

47 Part A of the existing Code applies to EFT transactions involving the crediting or debiting of an account maintained by an account institution. The clearest application of Part A then, is in relation to traditional banking products and transactions involving EFTPOS or ATMs. For transactions covered by Part A, the Code requires periodic statements showing transaction history to be provided, but more importantly makes the institution (and not the account holder) liable in respect of unauthorized transactions. Generally, banks (ADIs) and other traditional financial institutions are the subscribers to Part A of the Code.

48 Part B of the existing Code was initially designed to cater for newer products entering the market at the last review, which were stored value products. One example would be store-bought gift cards with a specific prepaid value. These were expected to be a major new growth area, but as they tended to be simple low-value products, a less onerous regime (Part B) was introduced to specifically apply to them. Requirements in Part A such as the provision of periodic statements or liability for unauthorized use do not apply as they are not mentioned in Part B of the Code.

49 However, the market has since moved to introduce products other than stored value products. Online payment gateway services such as PayPal and Paymate are commonly used worldwide, enabling consumers and businesses to transact with one another on the internet without providing the other party with their financial information.

50 The development of mobile payments in the past decade has given consumers new ways to purchase. For example, consumers can now pay for goods and services using text/SMS or application-driven services for smart phones.

51 Contactless transactions (using Near Field Communication technology) are also now available to give consumers the convenience of paying using their mobile phones, either by a chip placed inside the phone or a sticker attached to the case.

52 In Australia, many newer payment products have been developed and marketed using the angle of providing consumers with payment convenience, particularly for low value transactions. Some payment

providers minimise the potential losses arising out of fraud or unauthorised transactions by restricting the application of their new products or technology to low value transactions.

53 Many of these newer products could technically be covered by the definitions within the existing Part A (eg. transactions involving them may involve the crediting or debiting of an account). However, this would require those newer providers to comply with the more onerous Part A requirements even if the value and complexity of their product is relatively low. They would not be covered by the less onerous Part B as they are not stored value products. Consequently, many of the newer electronic payment product issuers have not subscribed to the Code.

54 On the other hand, some of the newer participants in the electronic payment market now offer products that are increasingly complex with relatively high monetary values that are accepted by a wide range of merchants. In effect, these products are capable of competing with traditional banking products in some sectors. It has been argued that this creates an uneven playing field between subscribers and non-subscribers to the Code because subscribers carry an additional compliance burden imposed by virtue of their Code subscription. More importantly, this leaves some consumers without the important protections embodied in the Code.

55 Some of the newer payment products are not subject to any specific industry code or regulations, even though (as noted) many have increasingly complex features and relatively high monetary values. For example, mobile phone payments (e.g. using SMS to pay for purchases) are not generally covered by a specific industry code or regulations unless they are classified as 'mobile premium services'. Consumers are often confused about how a transaction would be processed using new mobile payment methods, and have little appreciation about the associated risk.[11] Together, these factors increase the risks and potential losses for consumers should things go wrong.

56 We do not have comprehensive complaints data on non-traditional (including low value) electronic payment transactions. We receive complaints about providers of payment products from time to time; however, the overlapping nature of the products (e.g. mobile services being used as a payment product) does not always point consumers to ASIC as their immediate point of contact.

57 The Telecommunications Industry Ombudsman (TIO) received 13,899 complaints about mobile premium services in 2008, which increased to 15,653 in 2009. In 2010, new complaints to the TIO about mobile premium services decreased by about 70%, perhaps due to the tighter restrictions imposed by the Australian Communications and Media Authority in July

[11] See, for example, Australian Communications and Media Authority, 'Community research into attitudes towards the use of mobile payment services: Qualitative research report' (July 2010), p. 23.

2009. We are working with the Australian Communications and Media Authority to improve the effectiveness of the regulation of mobile payments.

58 Consumers are less likely to take the time to complain about something if the amount at stake is of low value.[12] For example, only half of the consumer respondents in the 'Australian Consumer Survey 2011' believe that a transaction involving $100–$150 is a significant purchase worthy of follow-up should a problem occur.[13] As such, the complaint figures collected by government agencies or external dispute resolution (EDR) schemes may not paint an accurate picture of the extent of problems in the low value payment market.

Objectives

59 The Code aims to provide adequate consumer protection for electronic payments to promote confidence in electronic payment products, particularly for products that have been introduced relatively recently.

60 To achieve this objective, the Code will be drafted and amended so that it is more technology neutral, flexible and attractive to payment providers. In this RIS we will focus on how the Code can be tailored for providers of low-value payment products to encourage newer payment providers to subscribe to the Code.

Options

61 We consider the options to meet the objectives for non-traditional and low value facilities (Issue 1) include:

Option 1: Remove Part B and revise the definitions used in the Code so the Code applies a single set of rules to all electronic payments.

Option 2*:* Remove Part B and revise the definitions used in the Code, but apply different rules to low value facilities (preferred option).

Option 3*:* Maintain the status quo.

62 As previously discussed, we do not consider making the Code mandatory for payment providers to be an option presently. We will strengthen our promotion of the Code and monitor the take up rate and effectiveness of the voluntary regime. If necessary, we will recommend a law reform in the electronic payment industry to the government.

[12] The Australian Government, 'Australian Consumer Survey 2011' (June 2011), p. 25.
[13] The Australian Government, 'Australian Consumer Survey 2011' (June 2011), p. 25.

Impact analysis

Option 1: Remove Part B and revise the definitions used in the Code so the Code applies a single set of rules to all electronic payments

Description of option

63 Under this option, Part B of the existing Code would be removed, leaving the standard rules (formerly Part A) to apply to all consumer electronic payment transactions. That is, there would be one set of rules applying to all electronic payment transactions.

64 The various definitions that are currently used to determine the applicability of the Code would be replaced with a single reference to transactions that are initiated using electronic equipment and not intended to be authenticated by comparing a manual signature with a specimen signature.

Impact on industry

65 Part B of the existing Code was designed to provide 'lighter' or less onerous requirements for stored value products which, in 2001, were a relatively new form of payment.

66 Part A of the Code, by contrast, was designed with the operations of the banking industry in mind. As such, it prescribes a much more stringent set of rules for subscribers providing products captured by Part A. Conventionally, as part of a prudentially regulated sector, banking products and services are subject to a higher level of regulation.

67 If Part B were removed, all subscribers would be required to comply with a stricter regime, regardless of the complexity and the monetary value of the product. Thus, a product issuer that offers only low value products with few product features would be subject to the same set of requirements to those who offer complex, high value payment products. This may discourage providers of non-traditional or low value products from subscribing to the Code.

68 More specifically, however, the removal of Part B and the imposition of Part A on all electronic payment products would have a slightly different impact on different industry participants. The impacts are summarised in Table 2.

Table 2: Impact of Option 1 on different industry participants

Industry group	Impact
Subscribers offering low value Part B products	Increased compliance costs through stricter Code requirements, including on terms and conditions; records of transactions and liability allocation for unauthorised transactions. Subscribers to update their staff and consumer documents, change operational practices and retrain their staff. Viability of this option would depend on the price structure of the product and the issuer's capital reserve.
Subscribers offering higher value Part B products	Similar impact to subscribers offering low value Part B products. Viability of this option would depend on the price structure of the product and the issuer's capital reserve. From a policy perspective, the impacts may be more acceptable for these products because high value products are likely to be more complex and pose more risks to consumers.
Subscribers offering low value Part A products	Code obligations remain the same. There might be improved long-term levelling of the 'playing field' in the market if similar products that were previously captured by Part B are subject to the same Part A requirements.
Subscribers offering higher value Part A products	Code obligations remain the same. There might be improved long-term levelling of the 'playing field' in the market if similar products that were previously captured by Part B are subject to the same Part A requirements.
Non-subscribers offering low value products	Less incentive to subscribe to the Code. Lack of knowledge would initially see consumers using these products, until something goes wrong and they realise that these products are not as safe as they thought they were. Consumer advocacy is gaining momentum and may lead to consumers leaving a product issuer en masse.[14]
Non-subscribers offering higher value products	Compared to non-subscribers who offer low value products, these issuers may have more incentive to subscribe to the Code. Issuers with a larger market share would be more affected by their decision whether or not to subscribe to the Code, due to their public profile and reputation.

69 Option 1 would be likely to impose more compliance costs on current subscribers, which may lead them to assess the tenability and the benefits of continuing their subscription.

[14] For example, one consumer website (www.vodafail.com) details the accounts of thousands of unsatisfied Vodafone customers. The compiled report has been submitted to the regulators and prompted the telecommunications carrier to take action to address the issues raised by their customers.

70 The compliance costs of Option 1 may also discourage non-subscribers from subscribing to the Code, particularly for product issuers who may not see the benefit of subscription outweighing the compliance costs and risk to their reputation flowing from their non-subscription to the Code.

71 On the other hand, the use of just one definition for the scope of the Code would simplify the application of the Code to subscribers and reduce compliance costs arising out of the different treatment of Part A and Part B products.

Impact on consumers

72 If current subscribers decide to continue their subscription to the Code (i.e. the main rules in Part A), consumers of electronic payment products overall would enjoy the same or more protection for their transactions. If current non-subscribers decide to subscribe to the Code, consumers of electronic payment products overall would enjoy more protection for their transactions.

73 However, it is likely that most current non-subscribers would decide against subscribing to the Code under Option 1 due to the compliance costs. It is not clear that they would be able to recoup these costs through higher prices. In this case, issuers of these products would continue to operate outside the ambit of the Code and their consumers would not benefit from the protection afforded by the Code.

74 It is also possible that current subscribers may decide to stop issuing low value stored products previously covered by Part B if they think it is not in their commercial interests to do so in light of the increased compliance costs from having to offer the same level of protection as Part A products. In this case, consumers may miss out on having access to useful payment products that were previously available to them. On the other hand, current subscribers may decide to withdraw from the Code if they think it is not in their commercial interests to remain in light of the increased compliance costs. In this case, consumers may miss out on having access to payment products with adequate levels of consumer protection.

Impact on external dispute resolution (EDR) schemes

75 Consumers of products issued by subscribers can complain about a breach of the Code to the subscriber. If a consumer is not satisfied with the outcome of their complaint, they can complain to an EDR scheme, such as the Financial Ombudsman Service (FOS) or the Credit Ombudsman Service Limited (COSL) if the subscriber belongs to a scheme. Not all subscribers are a member of an EDR scheme.

76 If Option 1 were accepted, EDR schemes would need to update their operational documents and train their staff who deal with complaints about breaches of the Code.

Impact on government

77 ASIC staff who deal with consumer inquiries and complaints would require training on the changes introduced by Option 1.[15] The number of inquiries and complaints is likely to increase under this option because fewer products are likely to have the protection of the Code and therefore more consumer problems are likely to arise. Some educational material would need to be written for our new consumer website, MoneySmart, and other audiences.

78 If, following the introduction of Option 1, more issuers decide to unsubscribe or not subscribe, the government would need to assess the adequacy of the self-regulatory regime for electronic payments. We would need to monitor developments in the market and Code membership.

Other impacts

79 Option 1 would also involve opportunity costs (or potential savings) to subscribers and non-subscribers to the Code, which would be lost through the decision to not allow 'lighter' requirements for issuers of low value products.

Option 2: Remove Part B and revise the definitions used in the Code, but apply different rules to low value facilities (preferred option)

Description of option

80 Under this option, Part B of the existing Code would be removed. The standard rules (formerly Part A of the Code) would apply to all payment transactions that are initiated using electronic equipment. However, different rules would apply to low value facilities.

81 In approaching the idea of a tailored regime for simple electronic payment products, we considered both how we should define 'simple products' and what kind of tailored requirements we should attach to them. These are interlinked issues; there is more than one to define a simple product, and what might be an appropriately tailored regime depends on how broadly or narrowly a simple product is defined.

82 In Consultation Paper 90 *Review of the Electronic Funds Transfer Code of Conduct 2007/08: ASIC proposals* (CP 90), we asked stakeholders if we could define simple products as a product that:

(a) cannot be cancelled by the issuer after it is issued;

(b) does not have an electronic authentication mechanism to safeguard consumers against unauthorised transactions; and

[15] We do not have records of the number of such inquiries and complaints.

(c) can hold a maximum value of $100 at any one time.

83 Submissions to CP 90 did not show any consensus on which products the tailored regime should be applied to. However, most submissions agreed that a less onerous regime should apply to certain types of electronic transactions.

84 Most submissions also argued that having the first two criteria in paragraph 82 would actually increase the risk of products being intentionally designed with less safety mechanisms so that they would captured by the 'lighter' requirements. This is not a policy outcome we want. We therefore made the policy decision to use a monetary threshold as the *sole* criterion for tailoring the requirements of the Code.

85 Our general approach to tailoring the requirements of the Code for these products was:

(a) the lower the monetary threshold, the more tailoring can be afforded to the requirements because the risks posed by very low value products will be smaller; and

(b) the higher the monetary threshold, the less tailoring can be afforded to the requirements because the risks posed by moderate value products will be more significant than it is for low value products.

86 In formulating the monetary threshold, we considered the current product offerings in the market. As a starting point, we need a threshold level that will maintain the Code's relevance to the market as newer products are becoming more sophisticated and capable of holding more dollar value.

87 The majority of submissions to CP 90 argued that a $100 threshold is too low. Alternatives submitted ranged from $250–$500 to $1000. Some of the submissions that suggested a $1000 threshold cited the need for consistency with the monetary threshold used in the *Anti Money-Laundering and Counter-Terrorism Financing Act 2006* (AML Act) and ASIC's Class Order [CO 05/736] *Low value non-cash payment facilities*. We do not consider these obligations overlap with the Code requirements or that the two thresholds need to be identical.[16]

88 We reviewed the regulatory treatment of newer electronic payment products in various overseas jurisdictions. Internationally, there is little consensus on how newer electronic payment products should be regulated. Relevantly, the UK and European Union have each adopted approaches that allow issuers of low value payment products to apply a 'light-touch' regime for product disclosure and liability allocation. See Appendix 1 for a summary of overseas approaches to the regulation of newer products.

[16] This approach is consistent with that of the UK, where the cut-off point for the lighter regime (€500) is lower than the threshold in the UK money laundering regulations (€2500 per calendar year).

89 As a monetary limit is the sole criterion determining the applicability of tailored requirements,[17] it should be set at a level that balances consumer and industry interests. Most consumers consider a purchase of $500 or more to be of significant value,[18] and that any losses involving a similar amount to be a significant detriment to consumers.

90 The tailored requirements would be available only to products with a maximum value of $500 at any one time. This threshold would capture many currently available products, particularly simpler products that pose limited risks to consumers. Users of products that can hold more than $500 should have the confidence from the knowledge that they are afforded the full protection of the Code.

91 The tailored requirements for low value facilities are summarised in Table 3.

Table 3: Tailored requirements for low value facilities under Option 2

Area	Tailored requirement	Full requirement
Terms and conditions	Subscribers have to give terms and conditions when it is practical to do so. Otherwise, subscribers must give consumers a notice that highlights key terms.	Subscribers must provide clear terms and conditions.
Reporting loss, theft or misuse	Subscribers do not have to have a specific process for consumers to report the loss, theft or misuse of a device, or breach of pass code security. However, subscribers must tell consumers *whether* they provide a process for doing this.	Subscribers must have a specific process for consumers to report the loss, theft or misuse of a device, or breach of pass code security.
Changes to terms and conditions	Subscribers do not have to give consumers advance notice of changes to terms and conditions unless they know the identity and contact details of the consumer. However, subscribers must publicise this information.	Subscribers must give consumers advance notice of changes to terms and conditions.
Receipts/ checking balances	Subscribers do not have to give consumers receipts. Instead, subscribers must give consumers a process to check their balance and their transaction history.	Subscribers must offer consumers a receipt for each transaction.
Periodic statements	Subscribers do not have to give consumers statements.	Subscribers must give consumers statements.
Liability for unauthorised transactions	The rules for allocating liability for unauthorised transactions do not apply to low value facilities.	Specific liability allocation rules apply.

[17] During the review, we considered other approaches to defining 'simple products' to which the tailored requirements would apply. This included products that cannot be cancelled if lost or stolen, and products that do not have an electronic authentication mechanism for safeguarding consumers against unauthorised transactions.
[18] The Australian Government, 'Australian Consumer Survey 2011', p. 29.

Impact on industry

92 Part B of the existing Code was designed to deal with stored value products because they were a newer form of payment. However, since its introduction in 2001, there have been no new subscribers to Part B of the Code.

93 Current subscribers who offer stored value products in compliance with Part B may incur some transitional costs when implementing the tailored requirements under Option 2. This may include monetary and time costs for changing disclosure documents and operational practices (e.g. developing complaints procedures that comply with the Code), as well as staff training on the requirements. Some costs may also be incurred in preparing notices for consumers that highlight key terms of the low value facilities and developing a process to allow consumers to check their balance and transaction history. However, most subscribers already have processes and resources in place to deliver these practices and features already, so additional costs due to the Code are likely to be minimal.

94 In CP 90, we asked for feedback from product issuers about the costs of complying with the tailored requirements. We did not receive any feedback from industry on this.

95 As no new firms have subscribed to Part B of the Code, we expect there to be no transitional costs for new subscribers to implement the tailored requirements. For current subscribers who may have used Part B for their stored value products, we expect the scope of transitional costs to be limited. Current subscribers would already have resources allocated to train their staff on the EFT Code, and we expect this arrangement to continue.

96 Currently 170 entities subscribe to the Code. The sizes of Code subscribers vary significantly across the spectrum. Bigger subscribers can be expected to incur more costs by the virtue of having more staff members to train and more disclosure documents to update compared to smaller subscribers.

97 Option 2 would mean that *all* products (not just stored value products) offered by subscribers that are $500 or less would be eligible for a tailored and more ‘light-touch’ regime. Currently, low value products other than stored value products are subject to a more onerous regime set out in Part A of the Code. The tailored regime, by contrast, would be a more flexible and lower compliance cost regime for all low value products, not just those of the ‘stored value’ variety.

98 Arguably, the above scenario would mean that some products under the value of $500 that are previously captured by Part A (accounts-based product provided by 'account institution' as defined in the EFT Code e.g. transaction accounts, credit card accounts) would come with lesser consumer protection measures under Option 2.

99 The above is a potential risk that we recognize. However, we believe it is more than outweighed by for the benefits of greater Code protection for more payment products. Furthermore, the Code will not prevent subscribers from providing a greater (Part A) level of consumer protection to their low-value products. Some subscribers may choose to adopt the same processes for all of their products (including low value products) as a matter of administrative simplicity, good customer service and to differentiate their products from their competitors.

100 For payment products offered by non-Code subscribers, the availability of a tailored regime will make subscription to the Code a more attractive and viable option. It makes the transition to becoming a subscriber a much easier process. Subscription by new payment providers to the Code would not lead to a trade-off between greater Code coverage and consumer protection in this case. Rather, it would provide consumers with additional level of protection when using newer payment products offered by Code subscribers.

101 We expect that any costs that subscribers may need to incur to implement Option 2 would be partially offset by the potential savings to subscribers across their product offerings because some of the participants in the low value product market would also be participating in the higher value market. For example, a number of banks have introduced contactless cards for low value, high volume transactions at premises such as convenience stores, fast food outlets and supermarkets.

102 Option 2 would also mean that Code subscribers who offer products that are capable of holding more than $500 would be subject to the more onerous requirements of the Code. Setting the threshold for tailored requirements at $500 might lead to some product issuers changing their product offering to under $500 only, and increase the competition in that market segment. We believe increased competition in the low value market is important to encourage innovation.

103 There may also be competition between low value products that are just under and over the $500 threshold. Issuers of products under the value of $500 would arguably gain a competitive advantage by qualifying for a less onerous treatment under the Code, even though there is arguably little difference between the products. However, this argument would arise regardless of where the monetary threshold is drawn.

104 Some submissions to CP 90 argued that consistency with the AML Act threshold would reduce the regulatory burden for industry participants. They also argued that the AML threshold was appropriate for the Code. We rejected this argument because the AML Act requirements have a different goal and purpose to those of the Code. While $1000 may be low value in the context of crime prevention (AML Act), it has a very different meaning in

the context of consumer protection. For this reason, the threshold set for AML purposes is of limited precedent value for the Code.

105 Our general approach towards tailored requirements is that the higher the monetary threshold, the less tailoring should be afforded to the requirements for these products. As such, the potential savings to current subscribers and non-subscribers from the tailored requirements would be less if the monetary threshold is set at $1000 rather than $500.

106 For example, if the threshold were set at $1000, subscribers that issue products capable of holding $1000 must provide consumers with the ability to cancel or suspend the product and obtain a refund of the product's remaining balance if the product is lost or stolen. In contrast, issuers of $500 payment products need not provide consumers with the ability to cancel or suspend a product, as long as they inform consumers of this.

107 Throughout the review and consultation process, we asked stakeholders for data on costs likely to be incurred by subscribers for complying with the tailored requirements and, specifically, how this varied depending on the dollar threshold. We did not receive any data on this.

108 It is not possible for us to come up with a reliable quantified estimate of the overall costs to payment providers who are non-subscribers to subscribe to the Code under Option 2. Newer payment providers do not typically publish information on the costs of their operations. New payment providers are a very broad and diverse group. Further, they are rapidly evolving, making it difficult to determine the size of the market held by these providers.

109 Considering the diversity of industry sectors and operational factors that are represented in the new payment market, it is impracticable to come up with a cost estimate that will reflect the operational reality of the vast numbers of different entities. In the absence of data provided by industry participants, a quantified estimation of costs would be misleading to the readers of this document. However, a qualitative analysis would point to a number of costs associated with the requirements put forward by the amended Code. Similar to existing subscribers to the Code, this may include monetary and time costs for changing disclosure documents and operational practices (e.g. developing complaints procedures that comply with the Code), as well as staff training on the requirements. Some costs may also be incurred in preparing notices for consumers that highlight key terms of the low value facilities and developing system processes to allow consumers to check their balance and transaction history. To the extent that these costs are not already being incurred to some degree (as may be the case with existing subscribers), these costs can be expected to be somewhat higher.

110 However, the voluntary nature of the Code means that a new subscriber will only subscribe if the benefits (e.g. reputational benefits and greater consumer

confidence in the provider) outweigh the compliance costs for that subscriber.

111 Some impacts of Option 2 would be quite similar to those of Option 1. For example, subscribers may incur costs for changing disclosure documents and operational practices, as well as staff training and complaints processes. Option 2 would also benefit industry in understanding its obligations under the Code with its use of a much simpler definition of the applicability of tailored requirements.

112 We have been in discussion with some newer payment providers about the need to consider their subscription to the Code. A number of these providers have responded positively to the inclusion of a tailored regime for products under the value of $500. We will continue to encourage payment providers to subscribe to the Code, and we expect a number of new subscribers to join the Code shortly and for existing subscribers to continue their subscription.

Impact on consumers

113 We are working towards improving the level of subscription by newer payment providers and anticipate that Option 2 would encourage providers of simple, low value products to subscribe to the Code. Currently, consumer recourse for some of the newer products is limited. In some cases, there are no legal protections. Subscription to the Code by more payment providers would enable more consumers to benefit from the protection afforded by the Code.

114 Low value payment products are useful to consumers. Option 2 would encourage payment providers to innovate in a way that maintains consumer confidence in the market (through Code-compliant products), without the onerous compliance burden.

115 Option 2 would mean that users of products offered by subscribers that are $500 or less in value would have a less comprehensive set of consumer protection measures where the product had been previously complying with Part A. Option 2 would not unreasonably reduce consumer protections compared to those currently afforded. As Table 3 shows, Option 2 would require subscribers to do certain things to meet consumers' needs, such as providing access to check their balance and transaction history.

116 We have considered the general features of low value products and the nature of use for these products in determining the appropriate requirements. For example, some of these products are used to purchase multiple, small-ticket items, for which consumers do not require a periodic statement. For this group of consumers, having access to check their balance and transaction history when they need it is generally sufficient.

117 Importantly, setting the monetary threshold at $500 limits the extent of consumer detriment that may flow from the loss, theft or misuse of such products. As mentioned previously, most consumer respondents in the 'Australian Consumer Survey 2011' consider purchases involving $500 and more to be significant purchases worthy of follow-up if a problem were to occur.[19] Consequently, consumers are likely to consider the detriment flowing from a loss greater than $500 to be significant.

118 Compared to products that can hold up to $500, products that can hold $1000 in value are usually more complex and have features that are more similar to banking products. In effect, they can act as a substitute for regular banking account products and therefore broader requirements (e.g. periodic statements) are required for these products. For example, products that are higher in value are more likely to be accepted by various merchants, rather than a single merchant.[20]

119 The risks to consumers of higher value products are not only limited to the risk of losing a greater amount of money. For example, some of the higher value products may be linked to the consumer's bank account for ease of reloading and account management generally. For these products, unauthorised transactions performed on the secondary product may increase the risk of unauthorised transactions performed on the bank account (depending on the design of the product and the strength of the system).

120 When consumer detriment is high, consumer confidence in newer electronic payment products may be diminished when things go wrong and consumers are unable to get recourse for their loss.

121 Consumers would benefit from Option 2 if the tailored approach leads to more payment providers subscribing to the Code. More subscribers would mean more Code-compliant products in the market, which would provide a greater level of protection for product users.

Impact on EDR schemes

122 We do not think the introduction of the tailored requirements would have much impact on the workload of EDR schemes. Under the tailored requirements, the rules for allocating liability for unauthorised transactions would not apply to low value facilities. Further, we understand the majority of low value complaints tend to be solved by the payment providers before they reach EDR stage.

123 Both FOS and COSL have been consulted during the review of the Code, with FOS actively participating in the drafting of the revised Code. Neither scheme has expressed concerns about Option 2.

[19] Australian Government, 'Australian Consumer Survey 2011' (June 2011), pp. 25 and 29.
[20] For example, Westpac MasterCard gift cards can hold up to $800 and can be used wherever MasterCard is accepted. In contrast, iTunes gift cards can hold up to $100 and be used for purchases at iTunes stores only.

124 Some of the impacts on EDR schemes would be similar to those of Option 1. EDR schemes would need to update their operational documents and train their staff who deal with complaints about breaches of the Code.

Impact on government

125 Under Option 2, we would need to train ASIC staff who deal with consumer inquiries and complaints. Some educational material would need to be written for our consumer website, MoneySmart, and other audiences.

126 We would monitor the development in the electronic payment market and subscription to the revised Code. If Option 2 did not lead to improved subscription by new, low value payment issuers and the market did not provide adequate consumer protection, we would, if necessary, recommend law reform to the government.

Other impacts

127 Option 2 would make the Code more attractive to payment providers that do not currently subscribe to the Code by giving them the option of complying with a 'light-touch' regime. We believe this would encourage greater subscription rates from these providers, which would significantly benefit consumers. It would also allow current subscribers who provide products capable of holding $500 or less to comply with the lesser requirements. This would help address the issue of an uneven playing field between subscribers and non-subscribers competing in the low value electronic payment market.

Option 3: Maintain the status quo

128 Under this option, we would keep the two-part approach of the existing Code. No concession would be given to low value payment products that do not use a stored value model.

Impact on industry

129 Low value payment product issuers that do not use stored value technology would have no choice but to comply with the full set of requirements (Part A) if they want to subscribe to the Code, regardless of the simplicity of their products. This may impose an unnecessary compliance burden on issuers of simple, low value products.

130 For example, many low value products are used to purchase multiple, small-ticket items, for which consumers do not require a periodic statement. For this group of consumers, having access to check their balance and transaction history when they need it is generally sufficient. To require issuers of these products to produce regular statements to users of these products (as Part A does) would impose additional compliance costs on issuers for minimal consumer benefit.

131 This may be why no stand-alone providers of stored value products have subscribed to the existing Code. There is no incentive for low value payment issuers to subscribe, particularly as it is voluntary.

132 When subscribers and non-subscribers are competing in the same payment market, industry participants argue that an uneven playing field ensues because the non-subscribers gain advantage through lower operational costs from not having to comply with the Code. Some subscribers may find that higher operational costs can be offset by the reputational advantage enjoyed by subscribers because consumers look for more credibility and protection. However, the lack of subscribers by non-traditional payment service providers to date suggests that this is unlikely to be a sufficient incentive for new subscriptions to the Code.

133 Subscribers that would like to reduce their compliance burden can only do so by designing their products to use stored value technology so as to qualify for the less onerous requirements. This would restrict product innovation in the electronic payment market.

134 Option 3 would involve opportunity costs for current and future subscribers to reduce compliance costs, which would otherwise be available for their low value products under Options 1 and 2.

Impact on consumers

135 Consumers of low value payment products offered by non-subscribers would continue to deal with any problems they may encounter with the products using predominantly the terms and conditions of the product issuer. There is an opportunity cost for consumers in missing out on the protection from potential subscribers who are not attracted to the existing Code.

136 We are aware of instances where product issuers do not follow best industry practice. Some terms and conditions fall short of the standards prescribed by the Code.

137 If the Code is unattractive, new payment providers will not subscribe to the Code. This would leave an increasingly big section of the consumer market whose payment transactions are not protected by the Code (or any industry code or regulations for some of the newer products).

138 In the worst case scenario, consumers may lose the level of protection already afforded by the Code if current subscribers decide to unsubscribe due to the issue of an uneven playing field.

Impact on EDR schemes

139 If the current two-part approach is maintained, the Code may remain unattractive to new payment providers who do not as yet subscribe to the

Code. Disputes involving non-subscribers may be more difficult and time-consuming to resolve because the specific rules in the Code (e.g. liability allocation) would not be available to deal with a complaint. The effect is broadly similar to that of Option 1, in that the requirements for allocating liability for unauthorised transactions would not apply to providers of low value products.

Impact on government

140 As the financial market regulator and administrator of the Code, we have the statutory objective to facilitate an efficient running of Australia's financial market, and promote the confident and informed participation by consumers in the market.[21]

141 To maintain confidence in the market and industry participants, the market needs a framework that enables consumers to obtain recourse when payment products or transactions go wrong. When the market is unable to provide recourse under the terms and conditions of its products, consumer confidence in payment products may diminish.

142 If low value product issuers decide not to subscribe to the Code because the compliance burden attached to Part A outweighs the commercial benefit, the issue of an uneven playing field among industry participants will remain.

143 If the status quo were maintained, we would be administering an industry Code that may have decreasing relevance and impact in an evolving payment market.

144 All these factors pose reputational risks to ASIC as the regulator of the financial market.

145 We would monitor the take-up rates of the Code and any problems relating to providers not subscribing to the Code, and assess the effectiveness of the current regime. If necessary, we would recommend law reform to the government to consider legislating or mandating subscription to the Code.

Conclusion and recommended option

146 To improve the relevance and effectiveness of the Code, the status quo cannot be maintained. The Code needs:

(a) a broad scope to include all electronic payment products; and

(b) a degree of flexibility that would allow issuers of simple products to subscribe to the Code and be subject to an appropriately tailored and

[21] ASIC Act, s1(2)(a)–(b).

less onerous regime, while still providing their customers with an acceptable level of consumer protection.

147 We have considered a number of factors in arriving at our recommendation, including:

(a) the complexity of the products offered in the market today;

(b) the potential for consumer detriment flowing from less than best business practice (for non-subscribers to the Code), as well as losses from fraudulent and unauthorised transactions; and

(c) the need for a more flexible framework in which providers can innovate their products and business practices.

148 After taking into account the benefits and costs of each option, we recommend Option 2.

C Issue 2: Mistaken internet payments

Assessing the problem

149 Internet banking services have revolutionised the way consumers make payments, and the use of these services has increased significantly in the past 10 years. Most authorised deposit-taking institutions (ADIs) in Australia now offer 'Pay Anyone' services as part of their internet banking service, where a person can transfer funds electronically to other account holders directly.

150 When using a Pay Anyone facility, a person is generally asked to provide the following information:

(a) the recipient's account name, Bank/State/Branch (BSB)[22] and account number details;

(b) the amount to be transferred; and

(c) text describing the transaction to the recipient.

151 Unfortunately, sometimes a person transfers funds to the wrong person because they enter the wrong payment details or because they have been given the wrong account information. Typically, the identity of the accidental recipient of the funds is unknown to the payer. There is no contractual relationship between the payer's ADI and the recipient of the funds.

152 Currently, there are no uniform procedures in the banking industry for recovering mistaken internet payments. The Australian Payments Clearing Association (APCA), the payment industry's self-regulatory body, has a number of provisions in its Bulk Electronic Clearing System (BECS) Procedures[23] that can be used to assist with the funds recovery process. However, these procedures are not binding on APCA members.[24] The procedures are confidential and the document is not available to non-APCA members.

153 ADIs are currently unable to retrieve money from an account without the consent of the account holder. This is the case even when the ADI has concluded that a mistaken payment has occurred and the money is still in the unintended recipient's account. It is therefore difficult for the payer to obtain their money back after it has been transferred to an unintended third party.

[22] This is a unique number that identifies the financial institution and the state and branch where the account was opened.
[23] BECS manages the exchange and settlement of bulk direct entry electronic low value transactions (e.g. an insurance company's direct debit arrangement with a large number of customers).
[24] Many, but not all, APCA members also subscribe to the Code. A list of APCA members is available at www.apca.com.au/Public/apca01_live.nsf/WebPageDisplay/About_Members.

154 We have received feedback from some subscribers to the Code about the difficulty they have experienced in having the counter-party ADI cooperate with them when dealing with mistaken payment complaints.

155 EDR schemes receive complaints about mistaken payments from time to time. When a dispute involves a payer and recipient of different ADIs, the schemes may be unable to assist if there is no direct relationship between the payer and the receiving ADI. Even when the scheme is able to hear a mistaken payment complaint, the disputed funds are sometimes hard to retrieve.

156 When a payer is unable to recover mistakenly paid funds using these procedures, they are left with the option of commencing a legal proceeding to determine the identity of the recipient. The costs of this exercise would often be prohibitive and exceed the value of the disputed mistaken payment.

157 In short, when a person pays the wrong recipient using the Pay Anyone internet banking facility, it is difficult for that person to recover the money.

158 Industry feedback suggests that mistaken internet payments are not currently a large problem. However, there is very little industry data to support this claim, or to show the extent of the problem, the causes of mistaken payments and the effectiveness of current methods used to recover them.

159 One of the difficulties ASIC faces as administrator of the Code is the lack of comprehensive data collection on newer electronic payment products. While we have anecdotal data to suggest that the problem exists, we are unable to obtain more data from industry participants because these data have not been systemically captured.

Liability for mistaken payments

160 During our early consultations on mistaken internet payments, some industry representatives raised the concern that if the Code were used to allocate liability for mistaken payments, it might be creating a new legal regime. Opinions diverge widely as to who should bear liability when the mistakenly paid funds cannot be recovered from the unintended recipient.

161 The right to recover a mistaken payment arises out of the doctrine of unjust enrichment.[25] A payer has a right to recover the money even if the mistake was caused by the payer's own negligence.[26] A payer may have a right to recover the money either from the unintended recipient or the recipient's ADI (acting as the recipient's agent). While the identity of the unintended recipient would normally be unknown to the payer, the identity of the receiving ADI could be ascertained more readily.

[25] *Pavey & Matthews Limited v Paul* (1986) 162 CLR 221; *David Securities Pty Ltd v Commonwealth Bank of Australia* (1991) 175 CLR 353.
[26] *Kelly v Solari* (1841) 9 M & W 54, 58–9; *Commercial Bank of Australia Limited v Younis* [1979] 1 NSWLR 444, 450.

162 While a payer has a right to recover a mistaken payment from a receiving ADI, the ADI will have an opportunity to establish a defence. In order to have a defence to the payer's claim, the receiving ADI must have passed the payment to the unintended recipient, without any notice that a mistake was made.[27]

163 Before the advance of electronic banking, a mere book entry crediting a person of the payment in question was not sufficient to displace the ADI's liability: the unintended recipient must have received the full benefit of the payment.[28] In contemporary banking, the point at which an ADI can be said to have truly passed on the payment is more unsettled. For example, an ADI may not have necessarily passed on a payment during the period between the recipient receiving a notice and the next transaction they make.[29]

164 We understand the BECS Procedures allow receiving ADIs to process a transaction based on account number details only. Some industry participants argue that any inconsistency between account name details and account number details does not constitute notice of a mistake because BECS Procedures allow receiving ADIs to process transactions using account number details only. The BECS Procedures, of course, are not law and therefore cannot affect any legal liability an ADI may have to a third party.

165 [Discussion on confidential BECS provisions omitted.]

166 When an ADI has some knowledge that a mistaken payment has occurred, equitable principles may apply to deem that a constructive trust may arise and that the ADI holds the payment on trust for the payer.[30]

167 As is the case in any civil litigation proceedings, the strength of a payer's case for recovering their mistakenly paid funds will differ depending on the facts of the case. Depending on the value of the amount lost, the average consumer will not consider instituting legal proceedings to recover their lost money.

Objectives

168 Our goal is for subscribers to (collectively) have an internet banking system that can prevent, as much as practicable, a mistake from happening in the first place, and to set out recovery procedures for recovering mistakenly paid funds.

[27] *Australia and New Zealand Banking Group Limited v Westpac Banking Corp* (1988) 164 CLR 662, 674.
[28] *Australia and New Zealand Banking Group Limited v Westpac Banking Corp* (1988) 164 CLR 662.
[29] *Australia and New Zealand Banking Group Limited v Westpac Banking Corp* (1988) 164 CLR 662.
[30] *Australia and New Zealand Banking Group Limited v Westpac Banking Corp* (1988) 164 CLR 662; *Wambo Coal Pty Ltd v Ariff* (2007) 63 ACSR 429; *Westpac Banking Corporation v Ollis* [2007] NSWSC 956.

169 Conventionally, the EFT Code is used to provide subscribers with clear and fair rules for allocating liability for unauthorised electronic payment transactions. We believe dealing with mistaken internet banking payments is also aligned with the above objective. It also aligns with the objectives to provide adequate consumer protection measures and procedures for resolving complaints and, ultimately, to promote consumer confidence in electronic payment products.

Options

170 We consider the options to meet the objectives for mistaken internet payments (Issue 2) include:

Option 1: Revise the Code to require an overhaul of the internet banking system and specify fund recovery procedures.

Option 2: Revise the Code to require some changes to the internet banking system and specify fund recovery procedures (preferred option).

Option 3: Maintain the status quo.

171 The question of how mistaken internet payments can be dealt with in the Code has drawn demarcation of opinions that were difficult to reconcile during the consultation process. We recognise that any solution to the issue will require significant compromises and cooperation by all stakeholders.

Impact analysis

Option 1: Revise the Code to require an overhaul of the internet banking system and specify fund recovery procedures

Description of option

172 Under this option, subscribers would be required to provide a Pay Anyone function that:

(a) validates BSB information entered by the payer and stops a transaction with invalid BSB information;

(b) requires the payer to enter the BSB and account information twice (while disabling the copy-and-paste function) and stop a transaction from being processed when the information does not match;

(c) validates the payee's account name information against the BSB and account number details, and stops a transaction with mismatched information; and

(d) delivers effective warnings about the risk of mistaken payments when a payer is performing a transaction.

173 The Code would also set out:

(a) where funds are available in the account, a recovery process for mistakenly paid funds based on how long after the mistaken payment the transaction is reported (see Table 4); and

(b) clarification of the role of EDR schemes in dealing with mistaken payment complaints.

174 If an ADI concludes a mistaken payment has not occurred, it would not be required to treat the situation as a mistaken payment. Consumers who are not satisfied with this outcome can complain to the sending ADI's EDR scheme. If the mistaken payment involves no direct relationship between the payer and the receiving ADI, an EDR scheme may still be able to hear a case brought by the payer provided that the receiving ADI consents to it. EDR schemes would issue guidance to clarify that an ADI can reverse a mistaken payment without the consent of an unintended recipient.

Table 4: Recovery procedures where funds are available in the account

Reporting period	Procedures
Mistaken payments reported within 10 business days of the transaction	The Code would provide that: • the sending ADI must investigate and determine whether a claim is a mistaken payment; • if satisfied a mistaken payment has occurred, the sending ADI must send a request for the return of the funds to the receiving ADI; • the receiving ADI must acknowledge a request for the return of the funds within 5 business days; • the receiving ADI will determine whether a request is a mistaken payment; • if satisfied that a mistaken payment has occurred, the receiving ADI must return the funds to the sending ADI, within 5 business days of receiving the request from the sending ADI, if practicable, or such longer period as is reasonably necessary, up to a maximum of 10 business days; • if not satisfied that a mistaken payment has occurred, the receiving ADI may seek the consent of the unintended recipient to return the funds to the holder; and • the sending ADI must return the funds to the holder as soon as practicable.

Reporting period	Procedures
Mistaken payments reported between 10 business days and 7 months of the transaction	The Code would provide that: • the sending ADI must investigate and determine whether a claim is a mistaken payment; • if satisfied a mistaken payment has occurred, the sending ADI must send a request for the return of funds to the receiving ADI; • the receiving ADI must acknowledge a request for the return of funds within 5 business days; • the receiving ADI must complete its investigation into the mistaken payment within 10 business days of receiving the request; • if satisfied that a mistaken payment has occurred, the receiving ADI must : – put a hold on the funds for a further 10 business days; and – notify the unintended recipient that it will withdraw the funds from their account, if the unintended recipient does not establish their entitlement to the funds within 10 business days commencing on the day the unintended recipient was prevented from withdrawing the funds; • if no substantiated claim is received within 10 business days, the receiving ADI must return the funds to the sending ADI within 2 business days after the 10 business day period when the funds are put on hold; • if not satisfied that a mistaken payment has occurred, the receiving ADI may seek the consent of the unintended recipient to return the funds to the holder; and • the sending ADI must return the funds to the holder as soon as practicable.
Mistaken payments reported after 7 months of the transaction	The Code would provide that: • the sending ADI must investigate and determine whether a claim is a mistaken payment; • if satisfied a mistaken payment has occurred, the sending ADI must send a request for the return of funds to the receiving ADI; • the receiving ADI must acknowledge a request for the return of the funds within 5 business days; • if the receiving ADI is satisfied that a mistaken internet payment has occurred, it must seek the consent of the unintended recipient to return the funds; • if not satisfied that a mistaken internet payment has occurred, the receiving ADI may seek the consent of the unintended recipient to return the funds to the holder; and • if the unintended recipient consents to the return of the funds: – the receiving ADI must return the funds to the sending ADI; and – the sending ADI must return the funds to the payer as soon as practicable.

175 If there are insufficient funds in the unintended recipient's account, ADIs must use reasonable endeavours to assist the fund recovery process.

Impact on industry

176 Option 1 would require most subscribers that currently provide a Pay Anyone function to undertake substantial changes to their internet banking system. For example, most institutions do not validate payee's account name information against BSB and account number information when processing a transaction. Instead, transactions are processed using BSB and account numbers alone.

177 This option would involve collective changes to payment standards. Subscribers would be required to implement a common set of standards about how BSB and account number information is sent and validated between financial institutions.

178 Industry representative bodies have argued that the costs involved in implementing Option 1 would be too high and excessive for the amount of mistaken payment disputes financial institutions receive. For example, one bank estimated in 2009 the cost of the implementation of all the proposals under Option 1 to be around $500,000.

179 The costs of implementing Option 1 would vary between subscribers. One bank estimated a cost of $200,000 for an IT system rebuild. This estimate would not address instances where the payments go to a wrong person because an incorrect but otherwise valid BSB number is used.

180 On the other hand, Option 1 would improve the robustness of the internet banking system. It would reduce the number of mistaken payments made by consumers, as well as the number of queries and complaints handled by the financial institutions resulting from the mistakes.

181 Lower incidences of mistaken payment complaints would lead to fewer complaints being taken by consumers to EDR schemes, and this would reduce the costs payable by subscribers to EDR schemes for dispute handling.

Impact on consumers

182 Under Option 1, some of the system changes would require consumers to do more when using a Pay Anyone function. For example, a payer would be required to enter the BSB and account information twice.

183 It was argued that more warnings in the payment system would simply cause consumers to 'switch off', and to revert to the approach most people take in responding to online disclosure. That is, a person will simply click on a button to express their consent without reading the terms and conditions.

184 We believe on-screen warnings, when properly designed and strategically placed, do encourage consumers to take more care in entering transaction details.

185 System changes would require some re-conditioning on the part of consumers as Pay Anyone users familiarise themselves with the changes. However, we consider the inconvenience to consumers minimal, and the benefit from Option 1 to outweigh any inconvenience.

186 Consumers would benefit from having a stronger payment system that significantly reduces the risk of losing money from mistaken payments.

187 Having a uniform recovery process would provide consumers with a clear expectation about the way in which their mistaken payment claim will be handled because the Code is a publicly available document.

188 The proposals under Option 1 were strongly supported by the consumer representatives in our Mistaken Internet Payments Working Group. In particular, consumer representatives argued the proposals to require subscribers to use a double-entry system for BSB and account numbers, combined with BSB validation and validating account number against account name details have the potential to significantly reduce the incidence of consumers inserting the wrong details when using Pay Anyone facility.

Impact on EDR schemes

189 Option 1 would reduce the risk of mistaken payments from happening in the first place. As discussed above, this would reduce the number of consumers complaining to their financial institutions about mistaken payments, and the number of complaints that eventually reach EDR schemes for resolution.

190 EDR schemes manage a high number of consumer complaints. Having fewer disputes to manage would improve the schemes' workloads.

191 Clear funds recovery procedures in the Code would also help EDR schemes to determine the cases before them (e.g. when giving consideration as to whether a financial institution has complied with the required procedures).

Impact on government

192 A more robust banking system is beneficial to the Australian government, and particularly to ASIC as the regulator of the financial market and administrator of the Code. We have the statutory objective to facilitate an efficient running of Australia's financial market, and promote the confident and informed participation by consumers in the market.

193 Under Option 1, we would need to dedicate resources to updating our printed and online resources relating to consumer rights for electronic banking, and train those staff who are likely to receive inquiries or complaints about electronic banking.

Option 2: Revise the Code to require some changes to the internet banking system and specify fund recovery procedures (preferred option)

194 Option 2 would require subscribers to:

(a) have an effective warning about the risk of mistaken payments to be delivered when a payer performs a Pay Anyone transaction;

(b) have a recovery process for mistakenly paid funds (see Table 4); and

(c) clarify the role of EDR schemes in dealing with mistaken payment complaints (see paragraph 174).

195 Option 2 would require the industry to collect data on mistaken payments for a period of three months. Among other things, the data to be collected would include:

(a) the number and value of mistaken payments;

(b) the causes of mistaken payments;

(c) the time taken by consumers to report mistaken payments; and

(d) the number and value of mistaken payments recovered and not recovered.

196 We would work with stakeholders to determine the details of the data to be collected.

197 Similarly to Option 1, if funds are still available in the unintended recipient's account, three fund recovery procedures can be applied by ADIs depending on when a payer reports the mistaken payment to their financial institution

198 Our general position for funds recovery procedures is that the sooner a mistaken payment is reported, the higher the likelihood that the funds will still be in the recipient's account and the easier the recovery of those funds.

199 If there are insufficient funds in the unintended recipient's account, ADIs must use reasonable endeavours to assist the fund recovery process.

Impact on industry

200 Option 2 would impose fewer obligations on subscribers (compared to Option 1) in exchange for agreement by subscriber ADIs to collect mistaken payments data for a three-month period.

201 Option 2 would only require subscribers to build an effective warning system into their internet banking system (if they do not have such a system already). This may involve subscribers revising existing warnings (or developing a consumer warning for those who do not already provide one) and making IT changes to deliver the message when a payer uses a Pay Anyone function. We do not have feedback from industry on how much it

would cost them to implement Option 2. However, this option was proposed to by industry members of the working group as an alternative to Option 1. Compared to Option 1, this option would cost subscribers a lot less to implement as it does not require subscribers to substantially change their internet banking system. As the option preferred by industry, we are confident that it is a far lower cost option for subscribers.

202 An effective warning system would benefit subscribers if it had the impact of making consumers generally more careful when transacting. This, in turn, would reduce the number of complaints received by ADIs about mistaken payments.

203 Under this option, the potential to reduce the incidence of mistaken payments is smaller than that of Option 1. Option 2 does not require subscribers to improve the design of their internet banking system to prevent the mistaken transaction from being processed.

204 The implementation of fund recovery procedures may involve some costs for subscribers to update their IT system and train their staff about the new process. While some components of this option might be relatively expensive to implement (e.g. IT system change), they will yield long-term benefits to subscribers.

205 The prescribed recovery procedures are expected to speed up dispute resolution times because the Code requires certain time limits to be met by subscribers. A faster dispute resolution process reduces the amount of staff time and resources that would otherwise be consumed by mistaken payment complaints. It would also give subscribers a better opportunity to repair the relationship with the customer involved in the mistaken payments claim.

206 We understand that the data collection process would impose some costs on subscribers. However, the costs would be less than the costs of implementing Option 1. We also believe the data collected from this exercise would help subscribers identify and understand the extent of mistaken payments in their organisation, particularly as this information has not been systemically captured by subscribers in the past.

Impact on consumers

207 The benefit for consumers of having an effective warning system has already been discussed in Option 1.

208 Option 2 does not require subscribers to make system changes to their internet banking system that would prevent mistaken payments from happening in the first place. Some subscribers might decide to go beyond the requirements of the Code, and make changes to the design of their internet banking system that would help stop a mistaken payment from being processed.

209 Other subscribers may not make the investment to improve their internet banking system, and users of Pay Anyone facilities will make a mistaken payment from time to time.

210 The fund recovery procedures would assist consumers in that they place an obligation on subscribers to handle a mistaken payment claim in a certain way and within a certain period of time. The Code also requires subscribers involved in a mistaken payment claim to cooperate with each other.

211 The three sets of fund recovery procedures reward consumers who take the care to check with the intended recipient about the receipt of funds, and take immediate action to rectify any mistake. The earlier a mistaken payment is reported, the swifter the recovery process will be. In the long run, we aim to improve consumer engagement with their financial matters. This approach is one of the many tools we can use to achieve this objective.

212 Consumer representatives were involved throughout the formulation of Option 2. This option represents compromises by all members in the Mistaken Internet Payments Working Group, and it is supported by all in the Working Group.

Impact on EDR schemes

213 Option 2 may not lead to a reduction in the number of mistaken payment complaints received by EDR schemes. However, the fund recovery procedures would help EDR schemes when determining a mistaken payment dispute before them (e.g. by giving consideration as to whether an ADI subscriber has followed the required recovery procedures).

Impact on government

214 Option 2 does not have as much potential to improve the robustness of the internet banking system as Option 1. However, it offers a uniform procedure that will help consumers recover their money in the event of a mistaken payment.

215 The ability for consumers to obtain recourse when things go wrong should improve consumer confidence in the banking system. This would assist ASIC in undertaking our mandate under the ASIC Act, among other things, to promote confident consumer participation in the financial system.

216 Similarly to Option 1, we would need to dedicate resources to update our printed and online resources and train those staff who are likely to receive inquiries or complaints about electronic banking.

Option 3: Maintain the status quo

217 Under Option 3, no action under the Code would be taken to address the issue of mistaken payments, and the current market arrangements would be maintained.

Impact on industry

218 Under this option, the prevention of mistaken payments and the funds recovery procedure are a matter of proprietary decisions for ADIs offering Pay Anyone internet banking facilities.

219 This option would give the most flexibility to ADIs as to how they deal with mistaken payments. ADIs can invest as little or as much resources in their internet banking systems as they choose. As Option 3 does not require subscribers to undertake anything, it is the cheapest option for ADIs in the short run. However, maintaining the status quo would mean existing issues (see paragraphs 149–167) would perpetuate in the market, at a cost to ADIs in the long run.

220 Option 3 would also involve opportunity costs to subscribers, with long-term cost-saving measures being forsaken (e.g. from having a system that is better at detecting and stopping a mistaken payment from being processed).

Impact on consumers

221 If the status quo is maintained, most internet banking systems will not detect incorrect payment details, nor warn consumers effectively of the risk of mistaken payments in a way that will prompt the payer to check their payment details before finalising their transaction. While most Pay Anyone facilities now come with a warning, the warnings are often delivered in very small fonts and in ways that are unlikely to come to the average user's attention.

222 If consumers were to rely on the existing arrangements, only a portion of mistakenly paid funds is likely to be successfully returned to the payer. [Confidential data omitted.]

Impact on EDR schemes

223 EDR schemes would continue to receive complaints from consumers who are not satisfied with the way their mistaken payment claim is handled by their ADI, or those who are not able to retrieve their funds under the existing arrangements.

224 As the payer does not usually know the identity of the funds recipient, the dispute is between the payer and the receiving ADI. In the circumstances where the mistaken payment involves no direct relationship between the payer and the receiving ADI (e.g. where the sending ADI, with whom the

payer has a direct contractual relationship, is not also the receiving ADI), a scheme may not be able to hear a case brought by the payer unless the receiving ADI consents to the process.

Impact on government

225 As the administrator of the Code, the decision not to take action to address the issue of mistaken payments would hinder our ability to make the Code as relevant to the electronic payment industry as possible.

226 Option 3 would also hinder our ability to fulfil our mandate to improve the performance of the financial system and promote consumer confidence and participation in the financial system.

Conclusion and recommended option

227 We recommend Option 2. Internet banking plays an important role in Australian consumer spending behaviour today, and its role is likely to increase in the future. We have identified some problems in the industry. The existing arrangements are not sufficient in preventing the incidence of mistaken payments or in rectifying the situation once the mistake has been made, and so maintaining the status quo (Option 3) is not an option.

228 The voluntary nature of the Code calls for consensus among stakeholders before any changes can be made to it. We are mindful of the potentially significant monetary burden on subscribers if comprehensive changes to the internet banking system were to be required.

229 The arrangements detailed in Option 2 are a marked improvement to the status quo, with some immediate and long-term benefits to the stakeholder groups involved.

230 Importantly, Option 2 has the support of industry groups as the party with most responsibility in implementing the change, and consumer representatives as users of Pay Anyone internet banking facilities. It will also provide ASIC and industry participants with more comprehensive data on mistaken payments complaints, which can later be used to evaluate the effectiveness of the Code provisions dealing with the issue.

D Consultation

231 The current review of the Code formally started in 2007 with the release of Consultation Paper 78 *Reviewing the EFT Code* (CP 78). CP 78 attracted over 40 public submissions from consumers and consumer bodies, financial service providers, industry bodies, dispute resolution bodies, academics and government agencies.

232 A second consultation paper, Consultation Paper 90 *Review of the Electronic Funds Transfer Code of Conduct 2007/08: ASIC proposals* (CP 90), was released in 2008. It consolidated the issues raised in CP 78 and contained proposals based on the feedback received to CP 78. We received 20 public submissions to CP 90, as well as some confidential submissions.

233 We have consulted extensively and comprehensively with stakeholders with interests in electronic payment products. Two working groups were formed to deliberate over issues surrounding the overall review of the Code as well as mistaken payments. Appendix 2 lists the members of both working groups. We also consulted with stakeholders involved in the innovative electronic payment product industry.

234 A list of public submissions to CP 78 and CP 90 is available at the Code webpage.[31] Table 5 below summarises the key issues raised in CP 90, submissions received and ASIC final position.

235 In December 2010, we released a report *Electronic Funds Transfer Code of Conduct review: Feedback on CP 90 and final positions* (REP 218). The report contains our final policy positions on the issues raised in this review. The report represents the broad consensus and support among stakeholders, as represented by the working group members, on the final positions taken.

236 The issues in this RIS have been analysed, debated and tested throughout the review and consultation process. The solutions proposed in this RIS reflect those of REP 218.

Table 5: Consultation issues, feedback from submissions and our final positions

Issue	Submissions	Final position
Statement of objectives The Code does not have a statement of objectives to provide clarity and guide interpretation.	All submissions support the inclusion of statement of objectives in the Code.	The Code will include a statement of objectives to explain the context and objectives the Code is designed to meet.

[31] See www.asic.gov.au/asic/asic.nsf/byheadline/Electronic+Funds+Transfer:+Code+of+Conduct?opendocument.

Issue	Submissions	Final position
Transactions covered by the Code The scope of the Code is currently defined in a complex and circular way. The application of the Code is broadly divided into account-based products and stored-value products. Electronic payment technology has moved beyond this dichotomy, and the Code needs to accommodate this.	Submissions broadly support the use of simpler definition and the use of non-exhaustive lists to clarify which transactions are and are not captured by the Code. A few submissions suggest wording or content changes.	The Code will include all consumer electronic funds transfer transactions initiated electronically. The Code will include a non-exhaustive list of examples of such transactions and a non-exhaustive list of transactions that are not covered.
Low value products regime The Code needs a light-touch regime for products that pose lower risks to consumers. A light-touch regime is needed to provide basic consumer protection mechanisms while promoting product innovation. Currently the Code offers a light-touch regime for stored value products only. Newer payment products have moved beyond stored-value technology, limiting the applicability of the Code in today's market.	Submissions broadly support the inclusion of tailored requirements for lower risk products. There are differing views on which products should be covered by the tailored requirements, and what the tailored requirements should be. Some submissions argue for the use of $1,000 monetary threshold for consistency with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML Act) and Class Order [CO 05/736] *Low value non-cash payment facilities*.	The Code will provide a light-touch regime for payment products that are capable of holding no more than $500 at any one-time (e.g. pre-paid gift cards and mobile phones), recognising that the risk to consumers from such products is lower than products that hold higher value. $1,000 is a significant sum for the average consumer. A lower monetary threshold is appropriate because the Code covers different protections to those of AML Act and CO 05/736.
Electronic disclosure Clarification is needed for the use of electronic communication in meeting Code disclosure requirements.	Submissions support the use of electronic communication for products covered by the Code. Some emphasise the need to obtain consumer's consent before electronic communication can be used. Others raised the concerns about the risk of 'phishing' attack through the use of hyperlinks.	Code subscribers can use electronic communication if the consumer consents to receiving information electronically. For products designed exclusively for electronic use, consumer consent can be obtained at the point of acquisition if this is made clear. For other products, electronic communication can be used when a consumer consents to receiving electronic communication and disclosure (opt-in). The use of hyperlinks will be discouraged for security reasons.

Issue	Submissions	Final position
Dispute resolution refinements Clarification is needed on various aspects of dispute resolution mechanism in the Code.	Submissions support the proposal that subscribers need not provide a consumer with written information about dispute resolution if the complaint is resolved to the consumer's satisfaction within a certain period. Submissions support having a limitation period for complaints to be determined in accordance with the Code, but opinions vary as to what the time-limit should be.	If a complaint is settled to the consumer and subscriber satisfaction within 5 business days, a subscriber is not required to provide written information about the outcome of complaint, unless requested by the consumer. If a complaint is not settled satisfactorily within 5 business days, the outcome and reasons for the outcome must be provided in writing. If an external dispute resolution scheme asks a subscriber to provide information relating to a complaint and the subscriber does not provide the information, the subscriber will have an opportunity to explain why it is unable to do so. In the absence of satisfactory explanation, the scheme can resolve a complaint based on the information available to it. The Code will introduce a six-year time limit for complaints to be brought to a subscriber for determination in accordance with the Code.
Liability for cards left in ATM The Code needs to clarify the liability allocation for situations where unauthorised transaction occurs as a result of a person leaving their card in an ATM.	Submissions broadly support the Code allocating liability to the consumer in this case, provided the ATM meets certain safety standards.	Consumers will be liable for losses resulting from them leaving their card in an ATM, provided the ATM incorporates reasonable safety standards to reduce the risk of a card being left in an ATM.
Book up Clarification is needed about what subscribers should do in relation to 'book up' practices.	Submissions support the proposal to require subscribers to prohibit merchants, using merchant agreements, from taking consumers' PIN as part of book up practices.	If a subscriber and a merchant have a merchant agreement, the agreement must prohibit the merchant from taking consumers' PIN as part of book up arrangements.

Issue	Submissions	Final position
Mistaken internet banking payments The Code does not currently deal with the issue of mistaken internet payments. Recovery of mistakenly paid funds from the unintended recipient has been difficult.	Initial stakeholder feedback was difficult to reconcile. An overhaul of the internet banking system to include mechanisms to minimise the risk of mistaken payment (e.g. BSB validation, cross-checking of account name and number details) will be expensive to implement. A fund recovery process should balance the interests of the payer, the unintended recipient and the financial institutions involved. Lack of comprehensive industry data on mistaken payments makes it difficult to gauge the extent of the problem.	The Code will deal with mistaken payments. Subscribers will be required to provide effective warning about the risk of mistaken payments to users of Pay Anyone facility. The Code will set out different processes for mistaken payment funds recovery (depending on how quickly the mistake is reported). The industry will collect mistaken payments data over a period of 3 months. ASIC will assess the efficacy of the fund recovery procedures after their implementation by subscribers.
Monitoring by ASIC Previously, Code subscribers were required to report on their compliance with every clause of the Code. This imposed significant compliance burden on subscribers. The data collected were also not comparable.	Submissions support the proposal to require subscribers to give ASIC data about unauthorised transactions, but noted the challenges involved in collecting comparable data. There is universal support for targeted compliance monitoring to replace the current monitoring system.	Subscribers will be required to provide ASIC or its agent annual information about unauthorised transactions. ASIC will consult stakeholders about the specific requirements. ASIC or its agent may also undertake targeted compliance monitoring of specific Code obligations..
Exemptions and modifications The Code currently gives ASIC limited powers to modify the application of specific provisions of the Code. A general power to modify the application of the Code is needed to enhance the flexibility and responsiveness of the Code.	Submissions support the proposal for ASIC to have a general power to modify the application of the Code to particular product or class of products. Some submissions argue that any modifications must be subject to prior consultation with stakeholders.	ASIC will have a general power to modify the application of the Code. ASIC will consult stakeholders before making any exemptions or modifications to the application of the Code.

E Implementation and review

237 We recently redrafted the Code in plain English, with the assistance of representatives from consumer, industry and EDR scheme bodies. We held a four-week public consultation process on the drafting of the new Code in May–June 2011. We aim to release the new Code around September 2011.

238 Subscribers to the existing Code will have 18 months to resubscribe and implement the new Code (including the preferred options discussed in this RIS), starting from the date that the Code is released.

239 The data collection exercise on mistaken payment complaints will help ASIC assess the effectiveness of the new mistaken payment provisions in the Code.

240 ASIC or our appointed agent will also monitor the effectiveness of the Code through annual compliance monitoring of subscribers' data on unauthorised transactions. We may also conduct targeted compliance monitoring of specific obligations under the Code.

241 The Code currently gives ASIC limited powers to modify the application of specific aspects of the Code. We have not used these powers to date. One of the issues we face as the administrator of the Code is the vast diversity of payment products offered in the market and the challenge in ensuring the Code's relevance in a constantly changing market.

242 Under the Code, we will have a general power to modify the application of the Code as it applies to a product or class of product. This general power could be exercised either upon application by stakeholders or on our own initiative. Before making any modifications, we must be satisfied that any consultation that we consider to be appropriate and reasonably practicable has been undertaken.

243 We will consider whether the modification is consistent with the objectives of the Code, and whether the application of the Code would be inappropriate and impose unreasonable burdens in the circumstances. We will also publish any modification made to the Code.

244 Finally, the Code will be reviewed every five years. If necessary, we may exercise our general power to modify the application of the Code in between periodic reviews.

Appendix 1: Overseas approach to regulation of newer products

245 We reviewed the regulatory treatment of newer electronic payment products in various overseas jurisdictions. Table 6 provides a summary of overseas approaches to the regulation of newer products.

Table 6: Overseas approach to regulation of newer electronic payment products

Country	Instrument	Scope and related requirements
Canada	EFT Code of Practice (due to be released)	Not available yet. Development of a new code remains on hold due to competing priorities.
European Union	E-Money Directive (Directive 2009/110/EC)[32]	The E-Money Directive defines 'electronic money' as monetary value stored electronically (including magnetically) for making payment transactions, which is accepted by third parties.
	Payment Services Directive (Directive 2007/64/EC)[33]	Electronic money products and issuers are regulated by the Payment Services Directive This directive provides a 'light-touch' regime for 'low-value payment instruments and electronic money' or products that store no more than €150 so that the issuer: • only needs to provide information about the main characteristics of the payment service; • gives only a reference to enable identification of a payment transaction, the transaction amount and any charges; • has options of not providing consumers with the means to notify the loss, theft or misappropriation of the product, or the ability to block further use; and • may let the user bear financial loss resulting from any loss, theft or misappropriation of the product if the issuer does not have the ability to block its further use.
United Kingdom	Electronic Money Regulations 2011(EMR)[34]	The EMR introduces a few new requirements for all electronic money issuers, including: • no time limits allowed on a consumer's right to redeem (though a fee may be charged for redemption in some cases); • consumers must be able to redeem e-money even if it is worth less than €10; and • electronic money institutions must safeguard money received from consumers and be able to repay consumers in the event of insolvency.
	Financial Services and Markets Act 2000 (FSMA)	The FSMA defines electronic money as monetary value that is stored on an electronic device, issued on funds receipts, and accepted as payment by persons other than the issuer as a surrogate for coins and banknotes.

[32] See eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32009L0110:EN:NOT.
[33] See eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:319:0001:01:en:HTML.
[34] See www.legislation.gov.uk/uksi/2011/99/made.

Country	Instrument	Scope and related requirements
	Payment Services Regulations 2009 (No. 209) (PSR)[35]	The PSR imposes business conduct requirements on all payment service providers, but applies lighter requirements for 'low-value payment instruments'. For products that store no more than €500, an issuer: • only needs to provide consumers with information about the payment service's main characteristics; • may provide consumers with simplified references to identify the transaction, the amount and any charges relating to the transaction; and • for anonymous products, must give consumers the means to check the amount of funds stored.
United States	Electronic Funds Transfer (Regulation E)[36]	Regulation E defines electronic fund transfer as any transfer initiated through an electronic terminal, telephone, computer or magnetic tape. It applies to point-of-sale transfers, ATM transfers, direct deposit or fund withdrawals, telephone transfers and debit card transactions. In March 2010, the US Federal Reserve Board amended Regulation E to implement the gift card provisions of the *Credit Card Accountability, Responsibility and Disclosure Act of 2009* to gift certificates, store gift cards and general use prepaid cards. The amendments include the rule that expiry dates for underlying funds must be at least 5 years after the date of card issuance, or 5 years after the date when funds were last loaded.
Hong Kong	Hong Kong Code of Banking Practice (HK Banking Code)[37]	The HK Banking Code contains requirements for stored value cards issued by banking institutions. The requirements include: • terms and conditions of accounts; • fees and charges of accounts; and • use of customer information. General Banking Code requirements also apply where relevant (e.g. when a stored value card can also be used as an ATM card).
	Banking Ordinance[38]	Non-bank card issuers of multi-purpose stored value cards are subject to the licensing requirements under the Banking Ordinance and the supervision of the Hong Kong Monetary Authority (HKMA). The HKMA encourages the industry to adopt a self-regulatory regime.
	Code of Practice for Multi-purpose Stored Value Card Operation[39]	The Code of Practice for Multi-purpose Stored Value Card Operation was issued by Octopus Cards Limited, the system operator of Octopus Cards. It is a voluntary industry code that employs a high-level principles-based approach to regulating multi-purpose stored value cards.

[35] See http://www.legislation.gov.uk/uksi/2009/209/contents/made
[36] See www.federalreserve.gov/bankinforeg/reglisting.htm.
[37] See www.hkab.org.hk/DisplayArticleAction.do?sid=5&ss=3.
[38] See www.legislation.gov.hk/blis_ind.nsf/WebView?OpenAgent&vwpg=CurAllEngDoc*155*0*155#155.
[39] See www.info.gov.hk/hkma/eng/bank/value_cards/code_of_practice_OCL.pdf

Appendix 2: Working groups

246 We consulted extensively and comprehensively with stakeholders with interests in electronic payment products. Two working groups were formed to deliberate over issues surrounding the overall review of the Code as well as mistaken payments: see Table 7 and Table 8. The Code has been redrafted in plain English with the help of representatives from consumer, industry and EDR scheme bodies: see Table 9.

Table 7: Members of the EFT Code Working Group

- ASIC (chair)
- Abacus Australian Mutuals
- Australian Bankers' Association
- Australian Finance Conference
- Australian Mobile Telecommunications Association
- Australian Payments Clearing Association
- Centre for Credit and Consumer Law
- Consumer Action Law Centre
- Department of Communications, Information Technology and the Arts
- Financial Ombudsman Service
- Galexia (on behalf of CHOICE and the Consumers' Federation of Australia)
- Telecommunications Industry Ombudsman
- Treasury

Table 8: Members of the Mistaken Internet Payments Working Group

- ASIC (chair)
- Abacus Australian Mutuals
- Australian Bankers' Association
- Australian Finance Conference
- Australian Payments Clearing Association
- Consumer Action Law Centre
- Financial Ombudsman Service
- Galexia (on behalf of CHOICE and Consumers' Federation of Australia)
- Law Council of Australia, Financial Services Committee

Table 9: Members of the Plain English Reference Group

- ASIC (chair)
- Abacus Australian Mutuals
- Australian Bankers' Association
- Australian Payments Clearing Association
- Chris Connolly, independent researcher (on behalf of CHOICE and the Consumers' Federation of Australia)
- Financial Ombudsman Service