Position statement on mobile commerce

10 January 2014

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer advocacy organisation
Suite 4.02, 55 Mountain St, Ultimo NSW 2007
Tel: (02) 9288 4000 | TTY: (02) 9281 5322 | Fax: (02) 9288 4019
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

CHOICE
57 Carrington Road Marrickville NSW 2204
Phone 02 9577 3333 | Fax 02 9577 3377
www.choice.com.au | campaigns@choice.com.au
The Australian Consumers' Association is a not-for-profit company limited by guarantee.

About this document

The principles set out in this document have been developed in consultation with ACCAN's members.

Background on m-commerce

Mobile commerce ('m-commerce') refers to payments and financial transactions carried out using a mobile device such as a smartphone or tablet computer. With the widespread uptake of mobile devices, the potential market for m-commerce has expanded, and as of early 2013 a number of Australian banks, retailers and communications providers are exploring their options for offering m-commerce services to consumers.

M-commerce can include a number of services. Banking using a mobile phone ('m-banking') is relatively widespread, with most large Australian banks offering mobile apps that provide various banking functions. 'M-payment' services can include premium SMS services, mobile billing services that allow users to charge purchases directly to their mobile phone account, and payments made at EFTPOS machines using Near Field Communication (NFC) chips that allow a mobile device to function like a contactless credit card.

Case study 1: mobile banking with ANZ's goMoney

ANZ's goMoney app[1] is one of a number of m-banking apps available in Australia. It allows the user to carry out most of the standard banking functions, including bank transfers, payments using BPAY, and account management.

Case study 2: electronic transfers with Bump Pay

The Bump Pay app[2] allows users to transfer funds to each other by physically bumping their smartphones together. The app detects the physical motion of the bump, and remote servers then determine which other phone felt the same bump—in theory, this will be the other person the user bumped phones with. Payments are made using the PayPal online payment system.

Case study 3: retail point-of-sale and transfers with the Commonwealth Bank's "Kaching"

The Commonwealth Bank's Kaching app[3] works with a special iPhone case containing an NFC chip to allow the phone to function as a contactless card at

[1] <http://www.gomoney.anz.com/>
[2] <http://bu.mp/company/labs>
[3] <http://www.commbank.com.au/mobile/commbank-kaching.html>

EFTPOS machines. The app also allows the user to make payments using the recipient's mobile number, email address or, most recently, their Facebook account.

Case study 4: vending machine payments using SMS messages

Coca-Cola is currently testing a range of systems for purchasing products at vending machines using a mobile phone.[4] One of these systems, being trialled in Norway, allows the consumer to make a purchase using an SMS message, with the cost of the product being added to the consumer's phone bill.

Case study 5: electronic money using Bitcoin

Bitcoin is a digital currency that aims to be secure and anonymous. Users can store "Bitcoins" in a digital wallet on their mobile device or computer, transfer Bitcoins to each other, and use Bitcoins to make purchases at a small but growing number of online and offline retailers.

Case study 6: Google Wallet and Gmail

Google Wallet is a service that can store information about a user's credit cards, debit cards, in-store offers, and so on.[5] This information can then be used to make purchases online or with an NFC-enabled Android phone. Google has recently announced that users of its Gmail and Google Wallet services will soon be able to send money through the Gmail system.[6]

Case study 7: ISIS

ISIS[7] is an organisation founded by US carriers AT&T Mobility, T-Mobile USA and Verizon Wireless with the goal of releasing NFC-enabled phones on a large scale. Unlike some other NFC phones, however, the security and payment information used for NFC transactions is included on an ISIS phone's SIM card and provided by the carrier. A smartphone app is still required to make transactions.

While the take-up of m-commerce in Australia has so far been relatively modest, the m-commerce market is likely to grow in the future.[8] M-commerce payments and transactions can be very convenient. By turning a smartphone into a mobile payments device, consumers can keep electronic records of their transactions, save themselves carrying multiple credit and debit cards, and make payments and purchases when and where it suits them.

---

[4] Coca-Cola, *Tapping into Taste: Pay With Your Phone at the Vending Machine*, 17 January 2013, <http://www.coca-colacompany.com/stories/tapping-into-taste-pay-with-your-phone-at-the-vending-machine>

[5] <http://www.google.com/wallet/>

[6] <http://www.google.com/wallet/send-money/>

[7] <https://www.paywithisis.com/>

[8] Ramli D, *Telcos risk being left behind in contactless payment race*, Financial Review, 29 April 2013, <http://www.afr.com/p/technology/telcos_risk_being_left_behind_in_kNVC5swyZDfSo0vvziOatM>.

However, m-commerce also brings a range of risks to consumers:

- Scam emails, websites, messages and mobile apps can be used to trick consumers into making m-commerce payments to the wrong people;
- Hardware errors can cause incorrect or multiple m-commerce payments;[9]
- Prices for items bought with m-commerce services can include a premium;
- It is relatively easy to lose or break a mobile device; and
- Mobile devices store an increasingly large amount of information about users—such as contact lists and locations—that can be accessed by apps.

Additionally, it may not always be clear to consumers where they should direct any complaints about m-commerce services, since there are multiple parties that might be involved in any m-commerce transaction—a problem could be caused by the retailer, their banks, the credit card companies, the app developers, the mobile device manufacturers or the communications providers. In order to have a complaint satisfactorily resolved, a consumer must potentially contact each of these parties, lodge an internal complaint, and escalate the complaint to an external dispute resolution body, where one exists.

[9] See for example Howard B, *Contactless 'charging errors' at Marks and Spencer*, BBC, 18 May 2013, <http://www.bbc.co.uk/news/business-22545804>.

General principles

Clear and simple regulation

Consumers need to be clear about the regulatory framework/regulators that apply to m-commerce. Multiple frameworks—for example, one set of regulations applying if a charge appears on a phone bill, another if a charge appears on a credit card statement—may lead to unnecessary complexity and confusion.

> *Explanatory note:*
>
> *The regulatory environment in relation to m-commerce is complex, with multiple laws and industry codes having potential application to m-commerce services and providers. For consumers, this means a lack of clarity about their rights, protections and obligations. While it is natural that multiple laws will regulate systems as complex as m-commerce systems, consumers will require clear guidance about the regulatory environment. This could be in the form of information targeted at consumers or a clear and accessible industry code or guideline.*

Enforceability

The regulations surrounding m-commerce systems must be enforceable with meaningful action, and must apply to all m-commerce providers. The mechanisms for triggering enforcement action must be accessible and affordable to consumers.

> *Explanatory note:*
>
> *A multitude of regulations will provide little consumer protection if those regulations are not enforceable. Any regulations applying to m-commerce must include mechanisms for action to be taken against a provider who fails to satisfy those regulations.*
>
> *Any regulations should apply to all relevant participants in m-commerce transactions. Voluntary industry codes and guidelines do not provide sufficient consumer protection, since there may be no obligation for a particular organisation to subscribe to the code or guideline, and no action possible against an organisation that violates the code or guideline.*
>
> *It is important that consumer action is available as a trigger for enforcement action. One mechanism for this is through the formal complaints process of an industry regulator.*
>
> *Whatever enforcement actions exist must be significant enough to encourage organisations to modify their behaviour. Formal warnings and non-binding determinations are not sufficient.*

Complaints and redress

Consumers should have clear and simple mechanisms for lodging complaints, disputing charges, notification of missing or stolen device or token and seeking redress or remedies for problems arising from using m-commerce services. Consumers must not be placed onto a 'complaint merry-go-round' arising from the multiple parties involved in an m-commerce transaction, and consumers should not 'fall through the cracks' between multiple complaints processes created by multiple regulations.

The avenues of complaint available to consumers should be readily identifiable, and information about these avenues of complaint should be provided to consumers in an easily accessible way.

These mechanisms could include a single resource for consumers to find out about their dispute resolution options, and free and independent dispute resolution through an external dispute resolution scheme.

Explanatory note:

M-commerce services involve a range of parties: a single transaction might involve the consumer, the retail merchant, each party's bank, a credit card provider, a communications network provider, a mobile hardware manufacturer, a mobile operating system developer and a mobile app developer. An error in an m-commerce transaction might be attributable to any one of these parties.

For consumers, this means uncertainty about their available avenues of complaint and redress. Depending on the nature of the complaint, it may appear to consumers that a complaint could be made to the bank, the communications provider, the retailer, the app developer, the mobile hardware manufacturer, the Telecommunications Industry Ombudsman, the Privacy Commissioner, ASIC or the ACCC. Clarity around the various complaint options is needed. This will in large part depend on the regulations that apply to m-commerce, and may depend on how consumers are billed for an m-commerce transaction: if a payment appears on their bank statement then complaint processes for financial matters may be appropriate; if a payment appears on their phone bill then complaint processes for telecommunications may be appropriate.

Clarity is needed around this point. Consumers need a clear avenue of complaint setting out who they should contact in the first instance, who they should contact if they wish to escalate their complaint, and what redress and remedies are available. This needs to be as straightforward as possible; consumers should not be forced to shop around for a complaints process because a transaction using a bank's m-commerce system appears on their phone bill, for instance.

Legal protections

Limited liability for unauthorised, delayed or duplicate transactions

Consumers must be protected from unintended transactions, and in particular from unintended transactions arising due to the nature of the technologies used in m-commerce transactions.

Consumers should not be liable for:

- Unauthorised transactions arising from fraud or negligence of a service provider;
- Unauthorised transactions arising from a malfunction of the technologies used in an m-commerce transaction;
- Incorrect duplicate transactions;
- Unauthorised transactions arising after the consumer reports an m-commerce device or token missing or stolen; and
- Unauthorised transactions in general where it is clear that the consumer did not contribute to the loss.

Measures should be taken by m-commerce service providers to limit the possibility of mistaken transactions and payments made due to some other error, such as accidentally triggering the payment process a second time. Consumers should not be liable for transactions arising in these ways unless they caused the transaction by, for example, telling somebody their password or failing to report a stolen card.

Consumers should not be held liable where a payment is unreasonably delayed for reasons outside the consumers' control.

> *Explanatory note:*
>
> *The ePayments Code currently provides some protections for consumers where an unauthorised transaction occurs if the consumer is not at fault. The protections of the ePayments Code extend to m-commerce transactions. However, while most banks, credit unions, etc., are voluntary subscribers to the ePayments Code, other participants in the m-commerce ecosystem—such as telecommunications providers—have not yet elected to subscribe to the Code. Equivalent protections are needed for consumers using m-commerce applications that are billed by their provider or other parties that are not bound by the ePayments Code.*
>
> *Consumers should also be protected against unreasonably long delays in processing payments—for instance, where a provider fails to process a payment for several days after it has been made by the consumer.*

Privacy

M-commerce systems should be subject to privacy impact assessments (PIAs), and the outcomes of these PIAs should be made publicly available.

M-commerce transactions should exceed the privacy protections of the *Privacy Act 1988* (Cth).

In the event that a provider, or any party with which it shares consumers' personal information, loses control of that information, the provider should notify all affected consumers, notify the regulator, and publish a notice (with personal information removed) on the provider's website. These notices must describe the circumstances surrounding the incident, the steps the provider is taking to limit the harm caused by the incident, the steps the provider is taking to prevent future incidents and the steps a consumer can take to minimise harm from the incident. Notification must occur as soon as practicable, with no unnecessary delay.

> *Explanatory note:*
>
> *Since m-commerce systems involve the use of personal information about finances they must be subject to additional privacy protections. To ensure that consumers have confidence in the privacy and security of m-commerce systems, transparent explanations of the ways in which personal information is collected, used, disclosed, and protected should be made available to consumers.*
>
> *Notification of data breaches provides an important consumer safeguard by keeping consumers informed of organisations' data-handling practices and by allowing consumers to take necessary steps when a breach occurs. A breach includes loss of control through unauthorised access (e.g. by an outside attacker or employee without clearance), unauthorised disclosure (e.g. making the information available on a public-facing website) or loss (e.g. leaving a USB stick with personal information on a train).*

No additional fees

Fees for using m-commerce services should be no higher than the fees charged for traditional credit cards or other payment systems. There should be no additional or increased fees charged on the basis that a transaction is carried out using an m-commerce system.

Any fees that are charged should be reasonable and related to the costs incurred by the provider for that transaction. Information about fees (including the amounts and the reasons for fees) should be made available to consumers in advance.

> *Explanatory note:*
>
> *Consumers should not have to pay extra for m-commerce—m-commerce is a tool used by businesses to generate revenue, and these businesses should not be able to justify a fee by dressing up m-commerce as something purely benefiting consumers. In particular, extra*

organisations in the m-commerce supply chain should not add additional fees—a telecommunications provider, for instance, should not charge a fee per transaction simply because the payment is made using their network, if the consumer already has a plan with that provider.

Technical protections

Authentication

Any m-commerce transaction must, by default, include an authentication step.

If authentication is to be skipped for any transactions (e.g. for low-value purchases at a point-of-sale terminal) the decision to skip authentication must rest with the consumer and must be made with free and informed consent.

A consumer's decision to remove authentication tests must not increase their liability for unauthorised or duplicate transactions.

> *Explanatory note:*
>
> *A number of contactless payment systems (in which a card or other payment device need only be held near a terminal for the transaction to continue) do not require any authentication of the user for payments below a certain value. This is usually marketed as a convenience for the user, who saves time by not needing to provide any kind of authentication code. However, the lack of any authentication step also presents a significant risk to consumers—if a credit card or m-commerce device is lost, an unauthorised person will easily be able to make payments using that card or device if no authentication is required.*
>
> *Consumers should be free to choose to take on the risk of unauthenticated transactions, so long as their choice is free and informed. A provider could optionally allow the consumer to specify the conditions under which authentication will not be required, e.g. for transactions below a particular value or to particular payees. An advantage of using computers and mobile devices for payments is that software can easily check whether these conditions have been met.*
>
> *A consumer's decisions to allow payments without authentication should not increase their liability. The decision to provide the consumer with the option of unauthenticated transactions rests with the provider, and a provider who is unwilling to take on the increased risk of unauthorised transactions introduced by the use of unauthenticated transactions should not provide this option to consumers.*

Security

M-commerce systems should implement security measures to ensure that users' personal and financial information cannot be accessed by unauthorised parties during transactions, while stored on the device, or while in transit. The measures need to include:

(i) Preventing unauthorised access to m-commerce apps;
(ii) Encrypting data stored on mobile devices;

(iii) Encrypting data in transit;
(iv) Limiting the range of times during which any payment hardware is active; and
(v) Protecting data stored on any providers' systems.

The security measures used by an m-commerce system must be disclosed to end users, at a level sufficient to make clear that appropriate measures are being taken.

Service providers involved in m-commerce transactions must take steps to ensure that consumers are aware of precautions that should be taken, such as the use of strong passwords or other authentication tools, how to avoid malware, and how to avoid scams.

> *Explanatory note:*
>
> *The information being used in m-commerce systems is highly sensitive. As well as financial information, it may include records of items purchased, identities of anyone the user transfers funds to, and locations where transactions are made. This information needs to be protected on the mobile device, on any servers used for the transaction, and in transit between all parties to the transaction.*
>
> *The hardware used to enable m-commerce may present additional security risks, and these must be sufficiently addressed. A "near field communication" (NFC) chip used to communicate between a mobile device and a payment terminal is, by definition, readable by remote devices, and this raises the risk of an unauthorised third party remotely reading the chip.*
>
> *Some m-commerce services also make use of third party networks to carry transactions. A notable example is Commonwealth Bank's 'Kaching' system,[10] which allows for transactions to be made over Facebook. This introduces an extra party to an m-commerce transaction, and it is important to ensure that Facebook (or any other third party involved in a transaction) is sufficiently securing the information they transmit and process. Commonwealth Bank notes a number of these security concerns on its Kaching website.*
>
> *M-commerce consumers also need to be aware of the more general security risks associated with mobile phones, such as the risks associated with scam messages, scam apps and phishing emails.*

Interoperability and technological neutrality

M-commerce systems should be interoperable. A consumer should not be unnecessarily restricted in the transactions they can perform because of their choice of mobile device, social network or financial institution. M-commerce systems should, as far as possible, not be dependent on a consumer having access to a particular technology.

[10] <http://www.commbank.com.au/mobile/kaching.html>

Explanatory note:

Some degree of vendor lock-in may be inevitable in the m-commerce market, and may be necessary to ensure that consumers' rights and protections are respected. One bank's mobile app should not provide access to another bank's account, for instance, even if the user is authorised. However, where it is possible, there should be interoperability between systems. A user should not be limited to making payments to people using the same mobile app, or through the same social network.

Some m-commerce systems will, by necessity, be connected to particular technology or devices. SMS payment systems, for example, can only work with a device capable of sending SMS messages; as of 2013, this function is generally limited to mobile phones. However, consumers should not be unnecessarily disadvantaged by their choices of technology. A second factor of authentication, for example, should be available to consumers of online banking systems who do not use a smartphone. Similarly, providers should make efforts to maximise the services available to consumers whose access to technology is limited due to their location, age, disability and so forth.

Marketing

Targeted advertising

Marketing and data analysis based on m-commerce transactions should be conducted on an opt-in basis. Consumers must explicitly consent to the use of their information for marketing and data analysis purposes. In order for consent to be free and informed, providers should clearly set out any organisation with which they will share personal information, and the reasons for this sharing.

> *Explanatory note:*
>
> *A record of consumers' purchase history is a useful tool for companies and marketers, since the purchases a consumer has made in the past are likely to be a useful guide to purchases they will make in the future. Credit card companies, loyalty programs, and online merchants already make use of these types of analytics, but m-commerce increases the types of data that could be used—location data showing where purchases are made, for instance, could be highly valuable to marketers.*
>
> *Modern 'big data' uses of personal information make it difficult for consumers to offer free and informed consent—it may not clear at the time the information is collected exactly what purposes it will be used for, and the frequency with which information is collected makes it impractical to request consent in every instance. Nevertheless, until alternative models of privacy protections are developed, free and informed consent remains and important requirement.*

Fair marketing and cooling off

Businesses and advertisers must be fair and reasonable in how they market to consumers. 'Hard selling' should be avoided, including advertisements that are 'pushed' to a user's m-commerce device.

'Cooling off' periods should offer protections to m-commerce consumers equivalent to the protections offered in other purchasing contexts.

> *Explanatory note:*
>
> *M-commerce allows a user to make purchases anywhere at any time. This makes consumers using m-commerce tempting targets for direct marketing—impulse purchases can be encouraged by clever timing of an advertisement.*
>
> *The Australian Consumer Law grants a ten day cooling off period for purchases made under an 'unsolicited consumer agreement', i.e. where the merchant contacted the consumer without invitation either by telephone or in person. This protection does not appear to apply*

to purchase made online, however, and this may exclude m-commerce transactions. However, an advertisement such as a pop-up browser window or SMS advertisement offering an m-commerce consumer a great deal—so long as they make their purchase within a short time window—should be subject to the same cooling-off requirements as the telephone or in-person cases.

App interface and functionality

Opt-in functions

M-commerce functions should be activated only where the consumer wishes to have those functions activated. Before new functions are activated for individual users, the provider must seek the free and informed consent of each user, e.g. by offering an opt-in option in a smartphone app.

> *Explanatory note:*
>
> *Introducing new features in an m-commerce system is in most cases a relatively straightforward matter of issuing an app update or adding a new section to an m-commerce website.*
>
> *New features can be useful, but they can also introduce new risks that individual consumers may not wish to carry. These risks might relate, for instance, to privacy (e.g. when an app introduces social media integration) or authorisation (e.g. when an m-commerce system no longer requires a PIN for transactions under a particular amount). Some consumers may welcome such functions, but others may not, and those who do not should not be forced to take on a risk that was not present when they signed on to a service.*
>
> *As a matter of best practice, even those functions that are available when a new customer signs on to the service should be activated only with free and informed consent, so far as possible.*

Accessibility

M-commerce systems must be accessible for people with disabilities and for culturally and linguistically diverse communities, where appropriate using internationally recognised standards such as the Web Content Accessibility Guidelines version 2.0. Accessibility functions should not detract from the other principles discussed above.

> *Explanatory note:*
>
> *M-commerce offers a relatively simple way for payment systems to be made more accessible. Apps can be developed with multiple language options, accessible interfaces, and functions such as text-to-speech to assist users with vision impairments.*
>
> *It is important that these features do not have negative consumer impacts in other ways. If an m-commerce app is available in multiple languages, the level of information in each language should be equivalent. If an app uses text-to-speech, sensitive information should not be automatically played through the loudspeaker of a mobile device.*

Spend controls

M-commerce systems should include functions to allow consumers to limit their spending by amounts, time, place, etc.

> *Explanatory note:*
>
> *Spend management is an important tool for consumers wishing to control how much they spend, where they spend it, what they spend it on, etc. Having the ability to do this is particularly important for consumers facing financial hardship.*
>
> *M-commerce systems operating on smartphones and other devices can easily accommodate such functions and provide the user with the ability to control the function using in-app settings.*

Record-keeping

M-commerce systems should provide consumers with a clear record of transactions, including the time and place of the transaction, the value of the transaction, the merchant or payee involved, the type of transaction (e.g. whether the transaction used NFC or a remote credit payment system), and whether or not the transaction was successful.

M-commerce systems should provide simple, legal recognised receipts. These might be generated from the transaction records kept on the user's device, so long as such records are recognised for the purposes of refunds, warranties, etc.

Since such records contain significant personal and financial information, it is crucial that the necessary privacy and security protections are applied.

> *Explanatory note:*
>
> *One of the advantages of m-commerce systems is the reduction in physical records they allow. As well as the convenience of not needing to carry printed receipts, the use of electronic records has positive implications for consumers keeping details of their transactions (for comparing with their banking records, for instance). However, it is important that these records have the same recognition as their printed equivalents, allowing consumers to obtain refunds and exercise their rights under warranties and consumer protection laws using electronic documents. Such recognition appears to be provided in Australia by the Electronic Transactions Act 1999 (Cth) and equivalent legislation in States and Territories.*