# Mobile payments and related parties, eg loyalty cards

September 2015

**Speed read**

Our article series on mobile payments explores some of the legal issues surrounding this new technology.

In this article we look to the future and focus on the commercial opportunities and legal risks facing loyalty programmes, innovators, and other service providers likely to work within or alongside mobile payments.

For example, loyalty cards like Flybuys can be expected to integrate with mobile payments platforms. Swiping two cards at the supermarket will be a thing of the past.


We list some useful questions related to privacy compliance, and note key issues as to B2B contracts between innovators and other providers on the mobile platform. For example, loyalty card providers will need to revisit their contracts with retailers, other suppliers, providers of data and probably banks, in this new world.

**The Detail**

**The story so far**

This article follows on from our earlier ones:

- *How does Apple make money from Apple Pay?*
- *Introduction to NZ mobile payments regulation and law*
- *Cybersecurity risk and mobile payments*
- *Mobile payments and the slippery slope of privacy loss…*
- *Retailers pay banks more over payWave/PayPass than over EFTPOS*
- *Mobile payments and competition law*

**A new consumer experience**

To date, mobile payment services have focused more on streamlining the payment process. But there is another objective rapidly gaining prominence: that of improving the consumer experience itself. Ancillary mobile payment services have the potential to significantly change our relationship with money and spending.

Here are just a few examples of this trend already developing in some mobile payments markets:

- **Integrated loyalty schemes**: Integrating loyalty within mobile wallet platforms would allow consumers to:

Mobile payments and related parties, eg loyalty cards

- automatically accrue rewards (without needing to carry or present additional loyalty cards at the point of sale); and
- aggregate a repository of total spending, guaranteeing that all purchases are rewarded. The NZ-based Semble is making moves in this direction, for example.

- **Personalised budgeting**: The detailed financial records retained by mobile wallets will likely enable apps to provide personalised budgeting advice while shopping, as and when consumers need it.
- **Capturing receipts**: Mobile wallets could also capture all the information necessary for evidential, tax, and financial records, replacing the need to retain paper receipts.

Existing success stories merely hint at the possibilities to come. The Starbucks app, for example, which is currently responsible for a whopping 7 million transactions each week, facilitates purchases and allows instant redemption of rewards and discounts at the point of sale. However, the closed-loop Starbucks app requires funds to be topped up, rather than being automatically drawn from an attached credit/debit card, and is not yet integrated into a wider loyalty or payment network (but this may happen soon).

**Opportunities and risks**

Given the other features already available on smartphones - location data, biometrics, multimedia access, and personal contacts, all updated in real-time - there is considerable scope for the development of innovative and interoperable mobile platform services.

Making the most of these commercial opportunities will require care as to legal compliance and managing risk. We address two key areas for mobile innovators: the B2B contracts between providers sharing a mobile platform, and wider privacy law issues.

**B2B contract issues**

A major issue for mobile payment innovators is defining their legal relationship with other businesses sharing the mobile payments platform, such as banks and merchants.

Loyalty providers, for example, currently deal with the rights and obligations of retailers participating in the programme. Integrating a loyalty programme into a mobile payments platform potentially adds more players to the mix, including banks, card schemes, and telcos.

What's more, the 'loyalty data' of an integrated service is more difficult to isolate (compared with separately swiping a Fly Buys card); information is now collected as part of the seamless, interoperable mobile payments service.

This raises some fundamental issues: which party legally holds this information? Who is responsible for protecting it? To what extent is each party liable for risk? Are consumers consenting to their personal information being shared between all parties? And if data is shared and matched, who owns the matched data?

Much will depend on the circumstances, the service provided, the potential overseas or cloud-based component, and the bargaining power of the parties. We canvassed a range of relevant ICT B2B contract issues in our six-part article series for the 2015 NZ Law Society IT and Online Law Conference, including Limitation of Liability clauses and the multi-jurisdictional nature of many modern IT contracts.

**Privacy law**

Another issue for mobile innovators is the privacy implications of collecting and utilising the personal information obtainable through a shared mobile payments platform.

In *Mobile payments and the slippery slope of privacy loss...* we discuss the rise of Big Data and the importance of privacy compliance.

Mobile payments and related parties, eg loyalty cards

The law is evolving to deal with the privacy issues created by new technology. Reform of the Privacy Act, for example, is expected to happen later this year. The NZ privacy regime is likely to be considerably strengthened; possible amendments include the mandatory reporting of data breaches, new regulatory investigation powers, and increased fines for non-compliance.

The Office of the Privacy Commissioner is also playing a role in this space, with regard to both monitoring non-compliance, and working alongside innovators to maintain privacy standards. The OPC began its 2014 report, *Making the Future: Working with business to create a smarter, brighter future for privacy*, by stating that:

> *"Innovators and businesses need to be able to develop and deploy emerging technologies in ways which realise the benefits without unwittingly compromising privacy values. This is where we can help."*

Privacy and data security remain an underlying consumer concern in the mobile payments space. The perception (and adoption) of robust privacy practices will likely increase the uptake of these services. Greater privacy compliance is evolving as a key marketplace battleground.

For example, Apple strongly market the fact they do not seek to use and aggregate personal information. They contrast their approach with that of providers such as Google and Facebook which build their business model on use and aggregation of customer data. The Googles and the Facebooks do this to offer free or low cost services to consumers, while using the data to attract revenues from corporates such as ad revenue. Consumers have to choose between, generally, cheaper but more intrusive services as against higher cost services that are not so intrusive.

Players in this market need to prioritise getting their privacy strategy right anyway, and work closely with experts to limit risk and maximise commercial opportunities. Regulatory intervention will likely undermine consumer trust and brand value (which the OPC acknowledges with its new power to 'name and shame', discussed here).

Judicial developments, imminent Privacy Act reform, and the renewed OPC focus on innovative technologies are all illustrative of the widening scope of legal risk and privacy liability when personal information is compromised. Aggregating and sharing data in innovative ways increases these risks.

In the context of ancillary services integrated with mobile payments platforms, privacy risk must be dealt with at a high strategic level, including data protection and cybersecurity (as we discuss here).

**Some useful privacy compliance questions for mobile innovators**

Here's a start on a list that can be more comprehensive and is dependent on the circumstances anyway:

- What information will be collected? Is the information anonymous, or can it be used to identify individuals? Is it necessary to collect all this information? The OPC's guidelines, *Need to know or nice to have*, helps mobile app developers understand the applicability of the Privacy Act in this regard.
- How will the information be used? Has informed consent been acquired? Does this consent sufficiently and specifically cover how the personal information will be used in practice? (The more the use of personal information is innovative and out of the ordinary, the greater the legal expectation that the terms are explicitly brought to the consumer's attention. This issue of incorporating contract terms will be important as increasingly novel mobile technologies are introduced to the market).

**Mobile payments and related parties, eg loyalty cards**

- Where is the personal information stored? Who owns it? And who can use it? Will the information be cloud-based, transferred overseas, or shared between providers? Which employees will have access to the information? Are there robust internal and external protocols to protect the information? We discuss this in more detail below.
- Attention will also be necessary as to the co-ordinated privacy and data protection standards maintained across the integrated system. As we noted here, security protocols and data management systems are only as strong as their weakest point.

**Wigley**+Company
PO Box 10842
Level6/23 Waring Taylor Street, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957
www.wigleylaw.com