18 August 2016

Email: adjudication@accc.gov.au

Ms Lyn Camilleri
Director, Adjudications
Australian Competition and Consumer Commission

Dear Ms Camilleri

RE: Bendigo and Adelaide Bank & Ors – Authorisation - A91546 & A91547
Submission of an Interested Party

Bluechain is a new entrant into the field of real-time secure, online and retail payments, and as such has a vested and substantiated interest in an ecosystem that is open to providing consumers, merchants and financial institutions the right combination of convenience, security and cost with the selection of payment solutions.

The founder of Bluechain was instrumental in the development of contactless technology for Visa completing Visa's first contactless trial in 2005 and the first live NFC trial in 2006 and development of Visa's payWave platform.

Today, through patented technology and real-time connectivity, it is possible to provide payment solutions with the appropriate level of security, without the requirement for single purpose secure hardware. However, what some emerging mobile payment applications require is the ability to interface with existing infrastructure, through interfaces on mobile devices such as contactless (NFC), Bluetooth and Wi-Fi. The Bluechain system can make use of, but does not rely on the contactless (NFC) interface to operate. The security architecture and mechanisms allow it to use any form of connectivity available (Bluetooth, Wi-Fi, Cellular Connectivity). With access to the complete range of NFC modes Bluechain is able to provide a more secure and efficient solution removing the need for single purpose devices, and opening up customer smart devices to a full range of services. Most Mobile Payment solutions today however rely primarily on contactless technology (e.g. NFC in slave mode) and existing contactless readers. These solutions also rely on hardware manufacturers of mobile handsets to provide unrestricted access to the NFC interface.

If the major Third Party Wallet providers and device manufacturers were to continue to selectively or completely lock control to alternate interfaces such as NFC, Bluetooth, Wi-Fi and biometric interfaces to third party providers would causing even more disruption to market choice. This would effectively constitute a case of using a position of market dominance to lock out or control competition.

As such, Bluechain supports the submission of the Consortium to enter into collective negotiations with Third Party Wallet providers to ensure compliance with industry best practises and principles and promote efficiency, transparency and open access to mobile hardware interfaces and banking

services between all parties. Ensuring an environment in which vigorous competition drives innovation, efficiency and continuing investment in payment solutions.

To underpin this, a short summary of the evolution of this multi-billion-dollar infrastructure is attached in the Addendum, and why access to interfaces is required. Bluechain is the natural next step in this evolution.

Regards

Craig Glendenning
CTO

Addendum

The evolution of Payment Technologies

There was a day, when EMV was considered modern…

This was 20 years ago. The first EMV specifications were named EMV1996 – they embraced a concept that was put in place in 1995. And, they addressed the problems that the payment system had at that time.

At that time, it was the answer to a problem that the whole industry had been looking for.

A step back in the history of Payment Cards:

Phase 1:
Card imprinters captured the details of the card holders via raised characters (embossing) on the card. The cards had security features to prove authenticity of the card, a signature was used to provide authenticity of the owner.
The imprinted paper slips were processed in a back office and settlement took a few days.

Phase 2:
Then came magnetic stripes that could store more information and cards were adapted to make use of this new technology. The physical card authenticity features remained, a few enhancements here and there (micro printing, UV printing, holograms).

At some point in time online systems came into play and that opened the potential for connection to a backend system to check legitimacy of the card and the cardholder (PIN), that had been introduced. Intelligent features such as PIN offset were added to the magstripe. This also meant that the onus of verifying the individual was put back to the terminal – it thus had to be secure. This was a paradigm shift in the evolution. The terminal now was the centrepiece of aggregation.

All this evolved over a period of 30-40 years.

But, cards could easily be cloned, and the online feature to get extra confidence meant a phone call @ 20c for every transaction – expensive and slow. Terminals were therefore still at the core of this technology.

Often people would come and say they need a 'card' that can do xyz – the answer was and still is: No, you need a system, the card is just the frontend.

Phase 3:
Smartcards were introduced to prevent cloning (to a limited degree SDA, to a high degree DDA). However, terminals did not really change, they were still the central aggregator of transactions and the common element. The EMV 1996 specifications were specifically designed to handle the constraints of the time (we did not live in a connected society, online commerce was just emerging).

Then came the internet, along with connectivity and associated web based commerce – EMV was never designed to handle this. Instead of fundamentally redesigning the system, the industry has looked at 'stop gap' measures to secure their investments and interests in what they had built - a

monolithic, static payment eco system that still relied on technology designed in the 90' to facilitate transactions in today's world.

To address the online systems that were emerging, the industry came up with standards such as SET (Secure Electronic Transactions) in an attempt to keep the existing system.

SET Features:
Personal Information remains confidential when making purchases
Cardholder Authentication
Merchant Authentication
Integrity of data

As of today, these are still the key elements that are required for a successful payment system – this has not changed, SET however was a system that was too complex for its time.

Phase 4:
The industry moved to cards that could operate in a contact or contactless mode (Dual Interface). Terminals followed shortly thereafter, providing the consumer a quicker and more seamless payment experience

Phase 5:
NFC interfaces were added to basic feature phones, to allow these to emulate cards, using embedded Secure Elements (eSE). Before this development could proliferate, smart phones were introduced which changed the way consumers went about their banking activities. As a natural next step systems were developed that allowed for security in the 'cloud'. The POS systems remained largely unchanged, yet again.

In a parallel development mobiles payments emerged in emerging markets, giving the previously unbanked access to cashless payments. Simple SMS based payment instructions could be sent in close to real time.

Phase 6:
Open communications and systems has given rise to unanticipated levels of Cybercrime. This billion-dollar infrastructure was again at risk, Tokenisation was introduced, adding complexity and further cementing the role of the traditional operators of this eco system. Technology lock outs started occurring such as mandates to use specific tokenisation services, and or restricting access to certain interfaces

And so we end up with the systems of today. Where to from here?

Phase 7: The seventh wave!

Systems will proliferate that bypass this monolithic, aging eco system that has served us so well for so many years. As much as we would like to hold on to this investment, the time has come to recognize that we can achieve the same results with a shift in thinking.

Bluechain does not reinvent the requirements, these have not changed. Bluechain makes use of today's technology to deliver a seamless payment experience.