Submission to the ACCC by Advanced Payment Systems Limited Against APCA's Reauthorisation

September 2009

Index

Executive Summary

Advanced Payment Systems Limited (APS) opposes the reauthorisation of APCA by the ACCC. APCA has abused its market power and has been responsible for preventing APS gaining access to the EFTPOS network for its mobile payment system over a number of years. APCA's action, along with the actions of its various committees, has occurred in spite of demand from the marketplace for the system and overwhelming evidence that the system is secure and conforms to the appropriate rules and standards from a number of independent experts.

This document details the lengths that APS has gone to in order to bring to the Australian market an EFTPOS innovation that is important for consumers, merchants and financial institutions. It also details the lengths that APCA has gone to prevent this deployment.

APS - formerly EFTWIRE Limited is a New Zealand registered software company specialising in the development of a mobile payments system based on the EFTPOS network. APS changed its name from EFTWIRE Limited in April 2009.

The APS technology is patented and is the basis of a Mobile Funds Transfer system, which has broad application in the financial services industry and represents a major innovation for the EFTPOS network. The system provides a mobile phone based payment platform, comprising of software and hardware, which acts as an intermediary between parties involved in mobile electronic transactions, for example financial institutions and merchants. A key benefit of the system is that it generates standard EFTPOS transactions into the banking network and requires no additional investment by the financial institutions. By using the system, consumers can make payments to merchants using their mobile phone to purchase goods or services, pay bills and pay for items purchased over the Internet. These payments are made without the need for the consumer to be physically present at an EFTPOS terminal.

While mobile payment systems are common worldwide, the normal process is for the payment to be applied the consumer's mobile phone bill or prepaid account or to use only card not present transactions for Scheme debit and credit cards. In the APS system the customer utilises a bank debit card and payment is applied to the consumer's nominated bank account using the standard EFTPOS network and processes. Scheme cards can also be processed, but this is not the focus of the system and they are currently out of scope in the current deployment. The system has been judged by a large number of independent experts to be extremely secure. This security is achieved because the system complies with all of the rules and standards relating to CECS and AS2805. Because the system is EFTPOS based, a fundamental requirement is for it to be able to connect to the EFTPOS network and send transactions to issuers for authorisation.

In order to use the system the consumer is required to perform a one-time registration, using their proprietary (bank) debit card at a standard APCA approved EFTPOS terminal, which contains a customised applet. During this registration information is securely captured and stored on the APS platform. This storage does not include or compromise the card PIN or sensitive cardholder data. The consumer is then able to use a mobile phone to send a text message to the platform from wherever there is mobile phone coverage, the message containing the mobile number, a Telephone Password created by the consumer during registration and a fund transfer request. The platform in turn builds a standard EFTPOS transaction in a standard APCA approved Host Security Module containing a special function call and obtains authorisation in real time from the relevant financial institution via the EFTPOS network, as though the customer had performed a normal EFTPOS transaction at a point of sale terminal. The removal of the physical card and EFTPOS/ATM terminal from the transaction eliminates the need for a consumer to be physically present at a merchant's premises to purchase goods or services. It also eliminates magnetic card minting or copying. It is an important innovation for the EFTPOS network.

The APS system has been deployed in Australia for a large merchant, has an acquirer prepared to accept transactions and has been fully tested and certified. It has been installed in two hosting sites in Sydney,

connected to a major mobile carrier's texting gateway and the acquirer's and merchant's platforms and is ready for production launch.

The development and implementation has involved the expenditure of several million dollars by APS, the merchant and the acquirer.

The first hurdle to obtain access to the EFTPOS network for a third party, non CECS member like APS is that APCA will only deal with issues bought by CECS members. This means that support has to be obtained from a CECS member before any real engagement with APCA can occur. This is in itself presented a problem, as APS had to obtain the support of a CECS member before it could fully engage with APCA.

However, once a CECS member had been recruited to act as the acquirer by the merchant in 2008, APCA management agreed to a clearly defined strategy with the acquirer to approve software for the devices that are an essential part of the APS system and for the acquirer to self certify the end to end system. APCA unilaterally changed this strategy after it became clear that the objectives in the strategy were going to be met.

The various APCA committees rejected applications to approve these devices in spite of the devices having obtained the required certification, as detailed in the CECS rules, from APCA's own Approved Evaluation Facility, Witham and in spite of independent experts confirming that the system is secure. These experts include Paymark (formerly ETSL), an international accounting and consulting firm, a renowned security specialist, the acquirer and a PCI QSAC.

The rejection has been based primarily on APCA/APCA committees deciding that the system stores the debit PIN, which contradicts the findings of all of the independent experts. This decision is convenient for APCA in that it has allowed it to interpret the CECS rules to decline the device approvals.

The system has also recently achieved PCI DSS compliance, which APCA has claimed is not relevant to CECs, but as this compliance involves a rigorous audit process, it does provide a useful measure of the systems inherent security. It also has confirmed that the PIN is not stored in the system. APCA does not have any comparable end to end system compliance procedures.

APCA is also arguing that the transactions are "card not present", in spite of the fact that the full Track 2 data and the PIN are presented as a standard EFTPOS transaction to the issuer for authorisation. Card not present transactions are not catered for within the CECS rules and this position also supports APCA's desire to create a new payment type, which can be seen throughout APCA's communications. APCA argues that the APS system breaches a fundamental principle of CECS because it does not require a cardholders to present their card and PIN directly at a Secure Cryptographic Device at the time of the transaction.

The fact that in the APS system, the cardholder presents their card and PIN at a Secure Cryptographic Device (EFTPOS terminal) during registration and then to perform a transaction, authorises the system to present their card and PIN via a secure Cryptographic Device (HSM), is totally ignored, as is the absolute security of the system. This process is the core of the innovation. Effective mobile transactions utilising the EFTPOS network are not possible if a cardholder has to be physically present at an EFTPOS terminal/ATM. APCA's argument is simply narrow minded and self serving.

As another justification for rejecting the approvals, while not stating it outright, APCA has suggested, without any supporting evidence, that the APS system might threaten the integrity of the EFTPOS network, while at the same time formally confirming in writing that "it has not identified anything in the internal security of the system that is of particular concern". APCA has also ignored all of the independent evidence that shows the system is totally secure.

In the case of the APS system, financial institutions do not have to make any investment for the system to provide benefits to their customers, both consumers and merchants. This is because the system

leverages off the existing EFTPOS infrastructure. It also leverages of the existing mobile phone infrastructure and as such, it is extremely efficient in economic terms.

However, financial institutions will receive standard EFTPOS fees for transactions from the system and issuers pay the acquirer. This is good for consumers and merchants, but not the issuers. The system therefore does not provide the commercial incentives that the financial institutions believe they are entitled to for a mobile commerce transaction or provide the control of a new payment channel that they believe is theirs by right.

Hence the financial institutions have been attempting to build their own mobile commerce system for a number of years that they can control and in the process derive higher fees. The APS system represents a threat to this strategy.

APCA's management were moderately supportive of the system following an RBA intervention late in 2008. However, the real power lies with the various APCA committees that are populated with employees from the financial institutions and there is no independent representation that mitigates the ambitions of interested and potentially conflicted parties. APS has been advised on a number of occasions that APCA committees are not independent from the member financial institutions and experience has proven this to be the case.

The APCA process over the past two years has resulted in another successful move by the financial institutions to block the deployment of the APS system, a situation that has been occurring since 2003.

The result of these deliberate actions by the financial institutions and APCA is that after nearly 6 years, the market still lacks an effective mobile commerce solution, consumers are being denied cost savings and convenience benefits and APS is facing the prospect of writing off its substantial investment in the system.

In addition, the merchant has made a large investment to deploy the system, as has the acquirer, with an expectation that it would go into production in November 2008. This expectation was based on the confidence displayed by the acquirer that APCA would not frustrate the process, providing that the system could be proven to be secure and the agreed strategy was followed. It was also based on APCA's initial input that approval would not be an issue providing certain processes were followed.

After APCA rejected the applications to approve the devices required for the system, the remaining option was for the acquirer to negotiate bi lateral agreements with each issuing bank. These negotiations commenced in January 09, but the merchant was not satisfied that this would meet its objectives and, after initially supporting approaches to a few banks, it withdrew its support for the project in August 09. That effectively ends the project and the infrastructure is now being dismantled.

Supporting Detail

The following is a detailed description of the events that support APS's submission and the information is in chronological order.

APS initially developed its EFTPOS based mobile commerce system in 2002 and 2003.

The system enables mobile phone customers to securely authorise remote, PIN based EFTPOS transactions from their mobiles in order to pay merchants. The system can be used by consumers to initiate many types of mobile commerce transactions, for example payment of bills, purchase of tickets, Internet payments and mobile prepaid top ups.

In 2003 this system was security audited by KPMG, examined and authorised by the risk and security groups of ASB, Westpac, National and BNZ in New Zealand and rigorously tested and certified by Paymark (ETSL).

APS began promoting its system to Australian financial institutions and merchants early in 2003. A number of the financial institutions' risk and security groups reviewed and found no issues with the system at this time.

APS also approached APCA in February 2003 and asked for an opportunity to present the system to it. The presentation took place with APS asking APCA for assistance. APCA formally advised that "it will be the responsibility of the Acquirer to advise APCA that the proposal meets the requirements defined".

APCA took an early stand that the PIN was stored in the system. This stand uses the following simplistic argument; as the PIN is used in the EFTPOS transaction sent to the financial institution for authorisation and the customer doesn't entered it into the mobile, it must be stored in the system.

The key to understanding how the system solves this dilemma is the registration process. During the registration the PIN is combined with the customer's mobile phone number and Telephone Password and then transformed through a special algorithmic process in a secure cryptographic device (EFTPOS terminal). Through this algorithmic transformation, the PIN data is fundamentally modified, so that the resulting data that is encrypted then sent to and stored in the system is no longer the PIN data. To prove the point, even if someone could decrypt this stored data, it is absolutely impossible to reconstruct the PIN. This can only be done by the system using an HSM, once the customer has supplied the phone number and Telephone Password and the algorithmic process, first performed during registration, is reversed. This non storage of the PIN is supported by the several organisations that have reviewed the system in detail and by the PCI DSS compliance recently received by APS for the system.

APS secured contracts with two major merchants in mid 2003, but after attempting and failing to gain access to the EFTPOS network over two years due to the concerted efforts of a number of financial institutions, APS withdrew its system from the market.

APS made renewed efforts to launch the service in Australia in 2007 after it became aware of the implications of the RBA's designation of the EFTPOS network.

APS approached a large merchant in July 2007 to determine if it was interested in a mobile commerce solution for its customers. The merchant discussed the system with a number of financial institutions and received some negative feedback.

Again the thrust from the financial institutions to the merchant was that the PIN is stored in the system and as this is not allowed under the regulations, it is not possible for the system to go into production. It was an easy argument for them to use, as without a good understanding of the processes that the system uses, it is difficult to grasp what is occurring in the system.

APS also discussed the system with one of the major financial institutions and the feedback on this occasion was positive, but an interesting position was taken by the financial institution.

There was a purposefully suggestion that the system provided a "card not present debit solution". There is no such thing in the CECS rules, but it is also consistent with APCA's approach to create a new payment type. Also of note was input from the financial institution that PCI DSS compliance of the system would create a positive impact. PCI compliance did not have the same impact on APCA, which has ignored the achievement and attempted to dismiss its relevance.

APS approached the RBA in 2007 to discuss the implications of the designation and came to the conclusion that providing due process was followed, access to the EFTPOS network could be gained.

On the RBA's advice APS met with APCA in August 2007 and APCA initially appeared to be co operative.

APS had introduced an organisation as a potential acquirer to the merchant in July, but the merchant preferred another organisation with which it had an existing relationship. APS continued to promote the first organisation, which emailed the merchant in September 07 to confirm its interest in acting as the acquirer. The organisation's comments are an interesting observation about the situation.

Extract from email:

I wanted to follow up our call of Tuesday and confirm our willingness to work with EFTWIRE to deploy a solution.

As you know, over several years, the major banks had failed to follow through their initial apparent commitments to sponsor the EFTWIRE solution into the Australian market. Given the economics of the situation this is not surprising, since institutions that issue credit cards will always have a conflict of interest in sponsoring EFTWIRE. EFTWIRE promotes the Domestic PIN based EFTPOS system, who's negative interchange is a cost to a card issuing bank. Further EFTWIRE has the potential to damage the major banks current very high margin on mobile top up sales through their terminals. Perhaps of most concern to other banks is that EFTWIRE can potentially allow a Telco to disinter mediate a bank's scheme card issuing business in the emerging M-commerce world.

As you will be aware, there have been regulatory and compliance changes in recent times that have made it possible to obtain the necessary approvals for the EFTWIRE solution without requiring approval from every issuer. New devices or equipment delivering CEC's compliant solutions now have to pass independent (approved) 3rd party lab certification prior to being installed into the payment system. There is no longer a need (or justification) for individual banks to do their own certification.

We see the EFTWIRE solution as a potential break through for the industry. We are keen to progress the EFTWIRE solution with you and believe that the path to implementation is now clear of obvious road blocks. We would therefore like to have the opportunity of presenting a proposal to you to acquire transactions generated by the EFWIRE system. We have been an early and consistent supporter of EFTWIRE and believe that we can deliver a high quality, low cost solution to you.

However, the merchant decided to contract with its preferred acquirer, which agreed to sponsor the system through APCA by self certification under the CECS rules.

In October 2007 APS sent APCA a detailed document titled "APS System Data Elements", which explained how the system worked in detail and also compared a transaction generated by the system against a standard EFTPOS transaction.

A meeting with APCA was held in October 2007, when APS went through the system using the document as a basis for discussions. APCA made it clear that addressing the storage of the PIM was a key issue.

Since CECs does not provide for an end to end system compliance process, APS decided to find an independent method to audit the end to end system to demonstrate to APCA that the PIN was not stored in the system and that the system was secure.
APS searched for an independent entity that could certify the end to end system and the solution came in the form of the compliance process established by the Card Schemes called PCI DSS, which is conducted by a Qualified Security Assessor (QSA) under the control of the PCI Security Standards Council. To obtain PCI DSS compliance, the end to end system is extensively security audited. One of the critical requirements for compliance is that the PIN cannot be stored in the system. This is exactly what APS was looking for to address APCA's concerns.

APS therefore engaged an international accounting and consulting firm to do the initial PCI scoping work and analysis prior to undertaking the full PCI compliance audit.

For the next 5 months APS continued to work with the acquirer and the merchant on the final specifications for the system and in March 08 APS and the merchant signed an agreement for deployment of the service for the merchant's customers. The merchant went ahead with this major commitment because it and the acquirer believed there was a clear route to gain APCA approval. Unfortunately this belief turned out to be incorrect.

Now that an agreement had been signed with the merchant, APS contacted APCA again in April 2008 to confirm the applicability of PCI to APCA in addressing the PIN storage issue.

APCA made it clear in an email reply to APS that PCI was not relevant to APCA and pointed out that a member needed to bring the issue of compliance to APCA. It also noted that;

"either the member needs to satisfy themselves, and specifically their internal auditor, that the system meets our rules and is prepared to sign off on this in their certification statement to us, or the CECS Management Committee has to make a specific ruling on this".

The email confirmed that the acquirer could self certify the system as an alternative to the CECS Management Committee approving it. However, APCA did not honour this commitment.

The acquirer then prepared a certification strategy document and sent it to APCA in April 08.
The key points of the strategy were that APCA would limit itself to approval of the terminal and HSM and the acquirer would self certify that the end to end system complied with all regulations. Also included in the strategy was that the major international accounting and consulting firm with experience of PCI would review the security of the platform with regard to Track 2 data storage and PIN storage.

The acquirer met with APCA in April to further discuss the process and later that day APCA confirmed in an email to APS that "This is a straightforward, inexpensive but important process and, assuming the implementation is secure, should not create any significant delays in your timeline."

The strategy required having APCA approve an EFTPOS terminal containing a new applet used for registration of customers within the system and also a standard HSM with a new function call developed for the system. The devices had to be added to the CECs approved devices list to be able to be connected to the network. This approval would follow certification of both devices by an Approved Evaluation Facility appointed by APCA for the purpose, namely Witham Laboratories out of Melbourne.

The strategy also confirmed that the acquirer would self certify the end to end system.

An email to the acquirer late in April confirmed APCA's agreement with this strategy. "We (APCA) are broadly in agreement with your certification strategy":

APCA's email also mentioned the review by the international accounting and consulting firm, which "should focus on compliance with the CECS Manual with particular focus on storage of the PIN".

However, this organisation had been engaged to undertake a PCI audit and not a CECS rules compliance audit.

APS subsequently asked this firm to confirm that the PIN is not stored in the system and this confirmation was provided. An email from it clearly states that "the system will not store sensitive authentication track and **PIN data**". This email was forwarded to APCA, but APCA disregarded it and recommended the acquirer use a respected encryption and security specialist to analyse the end to end system. This specialist was subsequently engaged to prepare a detailed report on the end to end system with particular reference to the CECS Regulations.

More importantly, APCA's email also referred to new CECS rules for storage of Track 2 data that were to come into effect in December 09. The email states that card holder data **"shall be protected in accordance with the requirements of the Payment Card Industry (PCI) Data Security Standard."**

This confirmation that the CECs rules will in future be using PCI DSS as a standard is in sharp contrast to APCA's claim only 2 weeks earlier, in the email to APS, that **"PCI is not relevant to APCA"**. Clearly, PCI is very relevant to APCA when it suits.

(APS engaged a PCI QSAC to undertake the PCI DSS compliance audit. This audit was completed in May 2009).

Based on the positive feedback from APCA, the parties then began the process of deploying the system and doing the work necessary to satisfy APCA's requirements.

Throughout, the acquirer kept APCA updated on the progress.

After several meetings and discussions with APS and the acquirer, the security specialist completed his analysis and issued a detailed report dated September 2008. The acquirer sent this report to APCA.

The report unequivocally states that the system is secure: **"No significant risk to PINs or card data was identified and no fatally bad risks were found in the proposed APS system"**. It also confirms that the system **meets the ATM and EFTPOS clearing rules contained in the CECS Regulations and Manual.**

As with all the other evidence that supports the APS system, APCA ignored the report.

Witham Labs in Melbourne examined the new HSM function call in September 2008, as per the strategy. The Witham report concluded that the function call did not pose any security issues for the EFTPOS network. As will be seen, APCA also ignored this report.

The Witham report was submitted to APCA in September with a request for the device to be approved as per the agreed strategy. APCA insisted on referring the HSM function call to its Technical Security Working Group (TSWG) for advice. However, based on the Witham report it was expected that this would be a rubber stamp exercise when the TSWG met on 22 September. Unfortunately, this did not transpire and the TSWG decided to ignore the report produced by APCA's own approved laboratory and other evidence and seek additional information on the system, thus exceeding its remit of approving/rejecting the HSM function call.

This additional information was provided to APCA by the acquirer w/c 20/10/08.

APS and the acquirer complained to the RBA about the difficulties being faced with regards to APCA.

A meeting was then requested by the acquirer with APCA management to go through the system in more detail. The security specialist and APS were asked to accompany the acquirer to the meeting. This meeting occurred on the 27 October and after a long debate APCA management agreed that the system was secure. However, it now said that the function call was not useful for any purpose and therefore APCA would not approve it. APCA also stated that the system was a paradigm shift and needed to be

cleared by the Standards Committee and MC3 in spite of this not being in the agreed strategy and in spite of APCA management knowing the nature of the system since at least October 2007 when detailed information was provided by APS. APCA also suggested that a rule change might be required and that this process could take up to 2 years.

The RBA spoke to the CEO of APCA in late October about what was occurring and expressed concern about access.

The acquirer and merchant met with the RBA on 31 October. APCA management were invited to attend, but declined because they were upset at the complaint APS had made to the RBA.

APS again wrote to the RBA about its concerns on 1 November and the RBA then arranged another meeting with APCA management and the acquirer on the following Monday.

At this meeting APCA management agreed that they had added additional elements to the strategy and after much discussion RBA, they finally agreed that APCA management would recommend the system to TSWG and MC3.

APCA management circulated a memo to the Standards Sub Committee members prior to the meeting which contained a recommendation that a limited trial be considered for the system.

In the memo APCA management reiterated its position that a transaction from the APS system is not an EFTPOS transaction and used a conflicting argument to support that position. It argued that the APS transaction did not involve the use of an EFTPOS Card at an EFTPOS terminal and that this made it clear, in spite of the fact that registration occurred using an EFTPOS card at an EFTPOS terminal, the APS transaction is not an EFTPOS transaction.

The whole point of mobile commerce is to remove the need for consumers to be physically present at an EFTPOS terminal to perform transactions and enable them to do so from a mobile phone wherever they are at the time. Rigorous interpretation of the CECS rules to define that an EFTPOS transaction can only occur by a customer physically swiping a card at an EFTPOS terminal will always result in a determination that a mobile phone initiated transaction cannot use the EFTPOS system as a transport and settlement process.

The TSWG and Standards Sub Committee met on 11 November with the acquirer and the security specialist in attendance. APS had been prevented from attending by APCA management. Scheduled for 45 minutes the meeting lasted for over 3 hours. The acquirer and security specialist's understanding was that the Committees would be addressing the HSM function call and only needed a high level description of the system. APCA management had full exposure to the system specifications and the acquirer knew that the recommendation was to approve a trial, which under the circumstances was considered a step forward.

The Committees obviously considered their remit extended beyond reviewing the Witham certification of the function call and wanted detailed discussions on the system itself, assuming the right to approve the end to end system and not just the function call. APCA management had not primed the acquirer that anything other than the function call would be discussed. The acquirer and security specialist had not expected this level of discussion and therefore were not prepared to answer members' detailed questions about the end to end system. APS was also not present to provide that input. In the words of one committee member, the meeting turned into a debacle and this gave the members the opportunity they needed to reject approval for the function call in spite of the Witham certification.

APS's absence from the meeting was a critical factor in the inability to answer these questions effectively and responsibility for this we believe rests with APCA management, as does the lack of clarity given to the acquirer and the security specialist about the expectations of the members to discuss the end to end system in detail. Prior to the meeting the members had not received the same detailed information on the workings of the system that APCA management had, and therefore had no basis from which to ask valid

questions, except regarding the function call itself. It was no wonder that the meeting had deteriorated into a debacle.

The TSWG and Standards Sub Committee decided not to approve the HSM function call and also not to recommend the system to MC3. No member supported APCA management's recommendation for a trial and they all voted against the system.

The members expressed "*Significant concerns with the system*", but these concerns were contrary to APCA management's views, the independent report from the security specialist, and the Witham report.

As the acquirer and security specialist later pointed out to APS and the merchant, there was no opportunity for the Committees' objections to be disputed and they were presented as a fait accompli.

The recommendation was also that MC3 urgently consider a project around a Card Not Present Transaction.

Card Not Present transactions do not use a PIN and by their very nature are less secure. However, as with credit card transactions that are card not present, the financial institutions can charge more because of the increased risk. In addition this recommendation provides an ideal excuse for further delay.

(As of 19 August 09, the acquirer was advised by APCA that a group has now been formed to investigate a new transaction type for Card Not Present transactions, "based on events of November last year". It has taken APCA fully 9 months to form this group under an urgent recommendation from the Standards Sub Committee.)

APS has major issues about APCA attempts to introduce this new transaction type, which it will try to use to categorise transactions from the APS system. Transactions from the APS system are Card Present with a PIN, the same as normal EFTPOS transactions. There is no increase in the risk or fraud potential compared to a standard EFTPOS transaction. The acquirer had previously recommended to APCA that it create a new transaction type to enable issuers to identify the APS transactions if the issuers wanted to do so. An interim solution to identify the transactions was also suggested for the medium term, so that the creation of a new type would not hold up the launch of the APS service. The acquirer also rejected the concept that the transactions be identified as card not present.

The APCA Management Committee (MC3) met on the 20 November where the acquirer and the merchant were better prepared and made a presentation to counter the points in the TSWG minutes and to ask for a 12 month trial to be approved.

A PowerPoint presentation was used to refute all of the reasons given by APCA for rejecting the system and requested a pilot be approved. MC3 refused the request

In January 09, APCA dealt with the second component of the system, the registration terminal application software, which was also certified by Witham Laboratories. No representation supporting the application was present at the meeting. As with the function call, APCA ignored the Witham certification and other independent evidence and the outcome of the Evaluation Review Subcommittee was as expected, i.e. the application for approval of the application software was declined on the basis of the use of a non standard PIN block.

APS have been challenging this since February 09 through a series of emails to APCA that show the reasons for the decline are not a correct interpretation of the regulations and furthermore that APCA incorrectly claims that the PIN is being stored in the system contrary to all the independent evidence that says otherwise. APCA was reluctant to respond to this input in spite of many follow ups by APS and the acquirer.

In May 2009, the PCI DSS compliance audit was completed and a compliance report supplied to APS.

The audit involved a comprehensive investigation of the system and a report on how the system meets over 100 requirements. Specifically, it confirms the international accounting and consulting firm and the security specialist's findings that the PIN is not stored in the system, which was the original objective for undertaking PCI DSS compliance.

APS emailed APCA on 19 June to advise it that APS had achieved PCI DSS compliance.
This compliance process represents a more rigorous analysis of the system by far than that undertaken by APCA.

APCA applied its consistent approach and ignored this input.

On 9 August, after APCA had failed over several weeks to respond to a number of emails from APS and the acquirer about the response required from APCA for the terminal application, APS called APCA to remind it that a response was overdue. APS received a blunt comment that a response would not make any difference. In addition, during the conversation, it was commented that APS's lack of presence at the various committee meetings at the end of 2008 didn't make any difference to the outcome. APS's response was that we had come to the end of the line and now had no choice but to make a complaint to the ACCC. (APS was unaware that APCA was authorised, but now understands how it can be so arrogant in its dealings with third parties).

On 11 August APCA finally provided a response on the terminal approval. APCA confirms: "Another, and perhaps more crucial area where we disagree in our ***interpretation*** [emphasis added by APS] is whether or not PINs are stored within the EFTWIRE system". It states that the CECS committee concluded that PINS are being stored, but also confirms that this is an 'interpretation". APCA makes no reference to the overwhelming independent evidence received by APCA that disagrees with the CECS committee's conclusion.

APCA also makes no reference to an earlier position, where it confirmed that there is "nothing in the CECS rules that contradicts the acquirer's position" that the PIN is not stored, but that "it goes against the **intent** of the system". Finally, APCA failed to mention that the committee members did not have access to a detailed and necessary understanding of how the APS system in order for it to make a reasonable decision on the matter.

APS then asked the acquirer to arrange new meetings with the various APCA committees as soon as possible, so that another attempt to gain approval could be made. However, with the cancellation of the project by the merchant, this serves no further purpose.

Glossary

APCA: Australian Payments Clearing Association. The Australian payments industry self-regulatory body. It is a public company owned by the financial institutions, building societies and credit unions.

APS: Advanced Payment Systems Limited, New Zealand registered company and until April 2009, known as EFTWIRE.

AS2805: The Australian Standard for Electronic funds transfer. It is near-exclusively used within Australia for exchange of financial messages between banks, ATMs and POS devices

CECS: Consumer Electronic Clearing System. CECS is a set of rules and guidelines that set minimum interchange standards to protect and enhance the security, integrity and efficiency of exchanges of consumer electronic payment messages.

EF50: Designation by APCA of the APS proprietary function call for an HSM.

ETSL: See Paymark.

EFTPOS: (short for *Electronic Funds Transfer at* Point Of Sale) is an Australian and New Zealand electronic processing system for credit cards, debit cards and charge cards.

HSM: Host Security Module. An HSM is a physical device in form of a plug-in card or an external security device that can be attached to general purpose computer and servers. The goals of an HSM are the: (a) secure generation, (b) secure storage, (c) and use of cryptographic and sensitive data material. HSMs provide both logical and physical protection of these materials from non-authorized use and potential adversaries. Also referred to as an SCM.

Mobile Payments: The payment of money by a consumer via a mobile device, such as their mobile phone, SmartPhone, Personal Digital Assistant (PDA) or other such device to enable the purchase of goods or services.

Passcode: See Telephone Password

Paymark: The major processor in New Zealand of retail electronic payment transactions. The company is owned by the major financial institutions. Formerly known as ETSL

PCI Security Standards Council: The PCI Security Standards Council (PCI SSC) is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc. The PCI SSC has issued the PCI DSS, a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

PCI DSS: A set of comprehensive requirements for enhancing payment account data security, issued by the PCI SCC to help facilitate the broad adoption of consistent data security measures and best practices on a global basis.

PCI QSAC: Qualified Security Assessor Company certified by the PCI SSC as being qualified to assess compliance to the PCI DSS standard.

Independent Security Specialist: An independent consultancy experienced in the data security and banking industries.

SCM: Security Control Module – see HSM.

Telephone Password: A code created by the customer at registration for the APS system and subsequently included in the customer's text message to authorise a transaction.

TSWG: Technical Services Working Group – An APCA committee comprised of CECS members charged with providing technical advice to other APCA committees.

Witham Laboratories: A leading independent provider of information security evaluations and offering **specialist consultancy** and **advice** in payment industry security. Witham is **APCA** accredited for bank evaluations in Australia as well as being a PCI QSAC.