Australian
Competition &
Consumer
Commission

FILE NOTE			
Matter name:	eBay International AG exclusive dealing notification N93365		
ACCC parties	Shane Chisholm		
Other parties	Greg Walter, CEO/Founder Qpay		
		Date	16/04/2008

Mr Walter called to provide an oral submission regarding this matter. Mr Walter is the CEO of Qpay, a competitor to PayPal.

Mr Walter advised that Qpay generally avoids offering its services to eBay merchants, as they have found that eBay merchants are often concerned about being cut off from using eBay if they acquire services from a competitor of PayPal. Mr Walter noted that Qpay currently only has one eBay merchant as a customer.

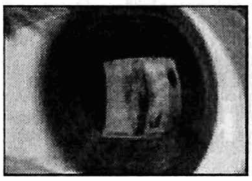
Mr Walter disputed eBay's claims regarding the notified conduct generating "security" benefits – in particular, that PayPal was the "most secure" payment method. Mr Walter advised that Qpay uses a tri-factor security system (involving mobile phone and PIN), and was able to use up to five factors, including automated voice, if required (further information regarding the system is set out in the attached white paper).

Mr Walter advised that PayPal primarily involved a one factor security system (ie a username and password), although it is introducing, for high end customers (although perhaps not in Australia), an additional security factor via a token, which generates a different code every 30 seconds. Mr Walter noted that this system was also not as secure as the systems offered by Qpay, due to the ability to determine the pattern that generates the codes by monitoring different entries, and the time between them.

Qpay Fraud Mitigation

Protecting your online activity – Anywhere Anytime. Qpay Fraud Mitigation provides advanced interactive Out of Band voice telephony security

Qpay's patent pending Fraud Mitigation addresses many of the challenges facing business, government and end-users when transacting online. Qpay Fraud Mitigation is a single intuitive solution that can interact with legacy systems and processes or operate standalone as a payments service with the Qpay Secure Mobile Wallet, to deliver confidence and financial stability.



Estimated at A$5 billion per annum the overall cost of fraud for Australia is almost 25% of the Total Cost of Crime according to the Australian Institute of Criminology. In 2004, the cost of ID Theft in the USA was estimated at U$54.6 billion at a cost to business of U$10,200 per incident.

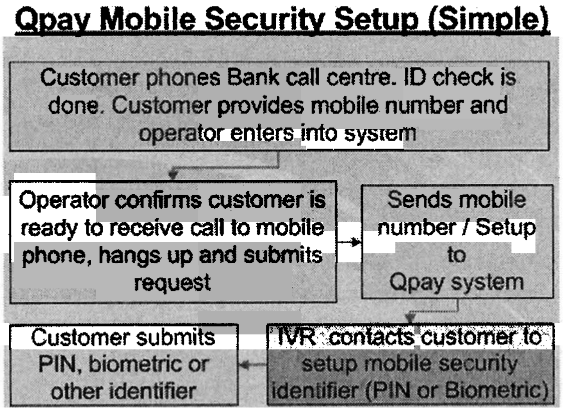
The Problem ~ A security solution is required that delivers equal to or better than Out of Band voice telephony at a price point similar to SMS messaging. The solution should be interactive and live, providing a real time confirmation by the user to authorise a transaction, highlight ID theft or fraud as the result of a root kit based Man-in-the-Middle attack.

With consumer confidence low for online serviceability and security, the solution must generate trust, a sense of control and be easy and universal to use. "*Banks potentially lose more money from a loss in consumer confidence in the online channel than they do from fraud losses*"[1]

What is Qpay Fraud Mitigation ~ An affordable, interactive, live service that places control back into the hands of the user. Focus is identifying the User not the Device. The User ID, authorisation and return path are all Out of Band. The solution operates on the user's own mobile phone regardless of type or carrier.

Operating to rapidly identify all fraudulent attacks including rootkit based man-in-the-middle, Qpay Fraud Mitigation is universal in application for secure logon services, internet banking, share trading, corporate network access controls, or to identify Customers who are registered with online merchant sites.

How it works ~ Once a transaction is initiated online from a users account, the Qpay system is triggered. Using a directive IVR user interface, Qpay Fraud Mitigation contacts the users registered mobile number and invites them to enter their PIN. The service relies on automated voice rather than SMS technology to deliver reliability and usability for all users. The response is also carried Out of Band and cannot be viewed via the internet.



Qpay Mobile Security Setup (Simple)

Customer phones Bank call centre. ID check is done. Customer provides mobile number and operator enters into system

Operator confirms customer is ready to receive call to mobile phone, hangs up and submits request

Sends mobile number / Setup to Qpay system

IVR contacts customer to setup mobile security identifier (PIN or Biometric)

Customer submits PIN, biometric or other identifier

The simple registration is intuitive and is not invasive to the end Customer.

[1] FFIEC Guidance Drives Online U.S. Banking Security Upgrades, Gartner report, January 2007

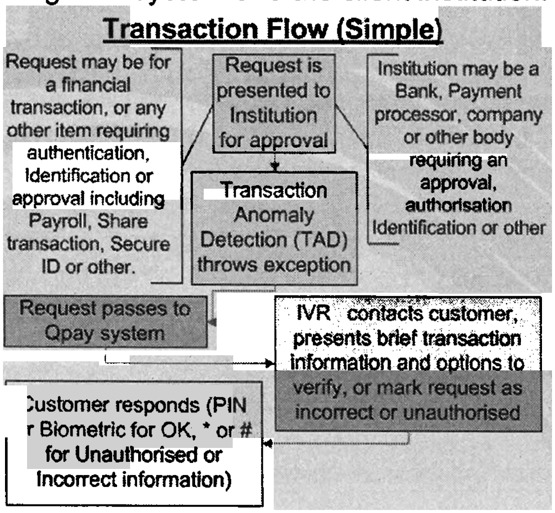
Considered features include:

***Unique ID between the systems* ~** Upon registration of a new user, the Qpay system generates a unique user ID. This ID is used thereafter to identify the user between the systems - as opposed to the mobile phone number. The mobile phone number only passes across the systems once upon registration - or if a mobile phone number change is initiated.

***Mobile phone number removal from User view and institution call centre view* ~** It is recommended that neither the user via the login, nor any institution call centre operator can view the attached mobile phone number.

***Hashing of data* ~** The user ID used between the Qpay and institution system, mobile phone number stored in the Qpay system and the user authentication (PIN or biometric file) are all triple DES encrypted.

The system supports a three-factor authentication model with full Out of Band operation and no passing of identifying Customer data between the Qpay Fraud Mitigation system and the client institution.


Transaction Flow (Simple)
Request may be for a financial transaction, or any other item requiring authentication, Identification or approval including Payroll, Share transaction, Secure ID or other.
Request is presented to Institution for approval
Institution may be a Bank, Payment processor, company or other body requiring an approval, authorisation Identification or other
Transaction Anomaly Detection (TAD) throws exception
Request passes to Qpay system
IVR contacts customer, presents brief transaction information and options to verify, or mark request as incorrect or unauthorised
:ustomer responds (PIN r Biometric for OK, * or # for Unauthorised or Incorrect information)

Multiple systems ensure higher security. Qpay takes the view that no single system can be guaranteed of being secure. The user's computer, the institutions systems, or the SIP connection can be compromised - a criminal may even set up a fake base station to catch information carried over the encrypted mobile channel. For a criminal to obtain a full data-set to perpetuate fraud, they will need to attack these multiple systems simultaneously.

The user experience ~ Engaging the Customer via their phone eliminates the need for a new device, and the Out of Band model addresses any security concerns with the phone itself. The IVR requests the user to confirm the transaction details and offers a limited range of responses and prompts which indicate any one of: Approved, Unauthorised or Man in the Middle attack.

Benefits delivered ~ With a view to secure more online activity, the benefits will extend beyond fraud mitigation.

How does it drive uptake? Studies have shown the mobile phone to be user's most trusted and reliable piece of technology today. PIN is a trusted form of authentication. While voice biometrics are not yet accepted by the broader community, it can be used to provide added security in the more sophisticated (and security sensitive) user space. As the user has a high trust level in a mobile phone / PIN combination, coupled with the opportunity to stop a transaction in its place, the consumer is in control and is more likely to transact.

Qpay Fraud Mitigation is a simple, visible and universal solution to cyber-attacks. It focuses on identifying the user and not a device as with many SMS and token based solutions that are exposed to friends and family fraud and do not always rely on something you know such as PIN.

A cost effective solution, Qpay Fraud Mitigation will let you focus on stopping fraud in its tracks, with the added benefit of renewing confidence in your online services.

For more information **Contact ~**

Qpay Pty Ltd
3/2 Pittwin Street North
Capalaba Queensland 4157
Phone: +61 7 3245 4066
Email: info@qpay.com.au