ACCC
Box 3131
Canberra ACT 2601
Attn: Darryl Channing
Email: adjudication@accc.gov.au

9 May 2008

Submission re: eBay International AG - Notification - N93365

The Cyberspace Law and Policy Centre is based at UNSW Law Faculty and has a charter to do research, education and advocacy in relation to public interest aspects of networked transactions. It is not a legal service or representative body, but engages extensively with a wide range of participants in online services and their regulation, including in the area of consumer digital rights and also IT security and malware.

Consultation period

We only became aware of the ACCC inquiry several days before the original deadline, after stories relating to eBay's Notification of Exclusive dealing were published in the media.[1] We are not in a position to fully address the many issues raised in this Notification in the short time available. Our various urgent attempts to discuss the concerns outlined below through eBay's web site channels, or by email to a known relevant officer, were not responded to in an interactive or effective way. We have potential access to expertise in banking, trade practices and internet law, but we would need a significantly longer consultation period to allow us to examine the full range of information and documentation, brief our advisers, and formulate detailed submissions. This short submission is thus based only on easily available material, and focuses on several main concerns, set out below. We are not in a position in the short term to ascertain the true factual basis behind some of these concerns, but consider that there is value in raising the concerns for further inquiry and investigation.

[1] *Australian Financial Review* IT section 29 April 2008, *The Australian* IT section 29 April 2008, ABC Radio National 'Law Report' 29 April 2008 c.8:30AM aest.

Detriments

Section 93(3) *Trade Practices Act 1974* places onus on ACCC to make findings in relation to the proposed conduct subject of the Notification, and inquire whether:

- The conduct is likely to have the effect of substantially lessening competition, and
- In all the circumstances, no public benefit is likely to result from the conduct, or any likely public benefit would not outweigh the detriment to the public constituted by any lessening of competition that is likely to result from the conduct.

The proposal to make PayPal the only means of payment (except COD) for all eBay transaction is in our view likely to have the effect of substantially lessening competition. There are a number of reasons including principally that substitution of another competing auction service is at this point in the evolution of the market for online auction and sales services, in Australia and internationally, relatively impractical, due to what we understand to be eBay's significant dominance of traffic, buyer numbers and items for sale. However we are not in a position to pursue this aspect further; we understand other stakeholders from a consumer and public interest perspective are making submissions in more detail, and we will take it as assumed that this element is met.

The issue before the Commission then is likely to become whether the public benefit is likely to outweigh the public detriments.

We do not propose to address the claimed public benefits in any depth.

We are instead concerned that there are several aspects of the proposal which may create new forms of detriment, in the form of reduced IT security and greater risks particularly for casual users, which should probably be taken into account. There are also some other issues we raise in relation to the role of sellers, and the potential for global effect of any decision in this case.

1. Potential that the new effective requirement for all eBay users to maintain and operate a Paypal account may create new security risks: to exacerbate susceptibility to spam-borne malware (especially 'zombie bot net' infections) and 'phishing' attacks propagated through fraudulent emails purporting to be from PayPal in relation to that PayPal account.

We understand that eBay contends the more or less exclusive use of PayPal will decrease the risk of "bad buyer experiences". In their Notification of Exclusive Dealing (NERA report) Report eBay outlined three types of "bad buyer experiences"

1) "fraudulent/unauthorised use of buyer credit card and/or account details where a method of payment has been used that involves disclosure of the buyer's account or credit card details;
2) purchased items not being received; and
3) purchased items being significantly not as described upon delivery"

It is the first that is of most concern to us. The forced switch to PayPal may not necessarily decrease the occurrence of these types of frauds. It may increase their occurrence. It may also increase some other sorts of fraud.

This is because many users who have not been exposed to the daily flow of PayPal email messages which they feel some need to open will be exposed to increased risks in this area for the first time.

PayPal does communicate to its users via email. PayPal sends users emails, including to inform them of the step they are at in the transaction process, and the steps they need to take to complete this process.

This means that the approximate 5 million current local eBay users (who will all need to now have PayPal accounts if they are to continue to participate in the largest online market) will need to start checking and reading emails from, or at least purport to be from, PayPal. It is this process of email communication between PayPal and its customers which puts the customers in a situation of increased security risk, because of the high and growing incidence of PayPal spam.

eBay users not using Paypal can safely and without thought routinely delete or filter out without reading all messages purporting to be from Paypal in relation to "their" account, by definition such as account does not exist and the message can be presumed to be a fake.

eBay users using Paypal, including those many who will be obliged to do so against their preferences under the new scheme, must assume that some of these messages are not fake. So they will now have to read and assess each one. This will result in many emails each day claiming to be from Paypal, perhaps hundreds each week or month per person, having to be read and assessed where now they are not read, just deleted. This is so even when a eBay member is merely a sporadic casual buyer, perhaps, as we understand, like the majority of such users, having only one transaction every few weeks or months.

So, in exchange for doing one online eBay transaction every so often, presumably among a number of other online transactions done with ordinary non-eBay vendors paid for by non-Paypal channels, all eBay users will now be required to accept a daily exposure to Paypal fake messages, which they are under some expectation to read. This is not the intention or 'fault' of Paypal of course, as they are no doubt engaged in attempts to mitigate or minimise such fraudulent abuses of the email system's vulnerability, but it is an intrinsic feature and implication of their proposal.

PayPal state on their website, by way of tools to help a user identify non-authentic messages allegedly from them, that they never ask for private details in email[2] (such as credit card numbers, Driver License numbers etc.).

---

[2] PayPal: Protect Yourself from Fraudulent Emails, http://www.paypal.com/cgi-bin/webscr?cmd=xpt/general/SecuritySpoof-outside. Accessed 29th April 2008

However, implicit here is the fact that the message must be selected and opened from the mail programs list of incoming unread messages, and the words and images read and assessed, thereby activating any 'web bugs' or image downloads embodied in it.

A non-Paypal customer does not have to open the message, and can delete it. While such deletion of unopened messages is not protection against all known malware infected email messages, it is several orders of magnitude less risky in IT security and human gullibility terms.

When a customer of any financial institution holds an account with that financial institution they are more or less obliged to check any emails that seem to have been sent by that financial institution. This is a problem because of the security vulnerabilities that are created with email usage, namely: phishing attacks and malware/zombie bot net attacks.

'Phishing' attacks

An email which purports to be from PayPal asks (in one form or another) for the recipient's personal PayPal account details, or, less commonly other significant information. Often the hoax email will send the individual to a website which looks exactly like PayPal's own website, and ask them to 'logon' – the whole process being identical to PayPal's normal 'logon' process. Rather than logging on to their account, the deceived user is sending their personal account information to the cyber criminal who sent them the hoax. Once the account details have been obtained the fraudster behind the scam may be able access the individual's PayPal account and utilise the funds therein, or obtain other benefits without authorisation.

These attacks are difficult to defend against, particularly for inexperienced Internet users or otherwise unsophisticated recipients.

If the end-user is educated about such attacks they are sometimes able to identify a hoax email. PayPal has information, above, on its website which informs users about how to identify such hoax emails.

But even sophisticated, literate and sceptical users are occasionally fooled by the ever-more convincing tricks. This is the human factor in IT security, and it has long been recognised as just as, or more, important than the purely technical aspects of IT security risk for end users.

Increased Vulnerability to PayPal Phishing Scams

eBay's 5 million users will now be obliged to operate PayPal accounts, which may have links to their credit card or other bank account details, or access to funds and transaction capabilities. This increases those eBay/Papal users' vulnerability to phishing scams, compared to an individual who does not hold a PayPal account and receives a hoax email claiming to be from PayPal, who does not need to open that email, or be tempted by any scams therein.

Malware attacks (especially infections by zombie bot nets):

Malware attacks, generally using mostly technical means, are often harder attacks to defend against than phishing. When a user opens the hoax email purporting to be from PayPal, an

inconspicuous piece of malicious software (malware) is installed on their computer, often at a very deep and almost ineradicable level. This software takes many forms, including a keylogger, which records keystrokes and sends this information to the perpetrator or others. This silent malware can monitor individuals inputting their credit card details, bank account details, passwords, and other sensitive information.

PayPal's consumer education can do little to minimise risk of this type of attack, which is on the increase in both severity and virulence, and is increasingly capable of self-mutation and other stealth technical tricks to avoid detection and removal.

Paypal recommend that hoax emails be detected by opening them and reading through them, hence detecting irregularities. But this is arguably triggering the main hazard with the other malware infected emails, which is activation of the malicious payload by the act of opening the email and 'executing' its contents.

The only way to minimise risk of such attacks is to only communicate with your consumers through secure internal sources (such as eBay's own internal messaging system), and to avoid obliging customers to read open unencrypted email messages from you.

Paypal is a particularly attractive target for spammers and malware senders because it is unusual in financial institutions in having a large user base in many countries. While there are similar attacks on customers of other institutions, the prospect that a random zombie-bot-sent message will find an actual customer of the targeted institution is orders of magnitude smaller than for PayPal. In addition the interactivity-intensive model of eBay sales is likely to mask fake emails more effectively than for plain banks, which have much fewer legitimate reasons to send messages. Fakes from banks stand out more, as the user does not expect so much 'chatter'. [3]

This new detriment, one way for risks to in fact be greater by the enforced use of Paypal compared to other transaction channels, should be one taken into account in assessing whether overall detriments are greater than the benefits.

2. The EFTPOS code of conduct will not apply to Paypal transactions; financial liability for losses incurred in phishing/ malware/ zombie-botnet scams is more likely be absorbed by individual users, rather than the institution (eBay/Paypal)

Referring to Annexure A s 5.5 (7) of the *Notification of Exclusive Dealing* (NERA) report that eBay International filed:

> (7) "PayPal offers additional buyer protection where an eligible item is not received or is "significantly not as described"."

---

[3] newsletter: 'PayPal Phishing Scam Exposed', http://www.whitecanyon.com/newsletter-paypal-phishing-scam-02-06.php; Antivirus: 'Scams target popular institutions', http://antivirus.about.com/cs/emailscams/a/bleBayscam5.htm; News.com: 'PayPal has fixed a flaw in its Web site to block a sophisticated scam designed to obtain sensitive data from members' http://www.news.com/PayPal-fixes-phishing-hole/2100-7349_3-6084974.html

It seems (by omission) that the PayPal Buyer Protection Policy (BPP) may not apply in all the of 'bad buyer experience' situations . It does not appear to apply where:

1) Fraudulent/unauthorised use of buyer credit card and/or account details where a method of payment has been used that involves disclosure of the buyer's account or credit card details[4]

This is the situation of most concern to us, because it is this type of fraud which is likely to increase due to the requirement that all eBay transactions be paid for through PayPal.

This may be in contrast with the EFTPOS code of conduct applying to many other financial institutions, which in Australia at least has support a balance in favour of the consumer in terms of liability for unauthorised transactions arising from IT security breaches at the user's PC.

3. Sellers: the practice of suspension of whole accounts inside PayPal represents a 'security' risk

Anecodatal evidence suggests there is common experience among sellers using Paypal of their whole account being suspended while a disputed transaction occurs. This is not typical of other financial transaction services.

There are claims by sellers to this author that the interface provided by PayPal is not responsive to the urgent need for resolution, as this can seriously harm an individuals attempts to use the system as a significant source of income, and can cause liquidity crises for micro businesses.

If sustained, the above practice of Paypal may represent an increased risk for those who at present use other transaction services.

The usage profile of eBay is such that the distinction between buyers and sellers is indistinct. Many consumers are also casual vendors. Many small vendors seek to develop into more robust small businesses. This is inherent in both the Web 2.0 interactive model of which eBay is an early exemplar, and of auctions.

While presumably eBay protective services, including those which are claimed to be the benefit offered by the transition to Paypal, do rely to some extent on the discipline possible through the mechanism of suspensions, more investigation is required to establish whether in practice the routine mode of use of this approach is proportionate to the harm addressed, and thus whether or not it does in effect pose an extra and unnecessary risk for small sellers.

Credit cards are used for many online transactions. Anecdotally the incidence of ordinary credit card fraud online is very low, probably below 1% of total transaction value, possibly below 0.1%. (We do not have estimates for other payment channels to hand, but only one alternative need be viable to undermine claims that Paypal alone is essential.) It is unclear how the PayPal-only scheme could be less risky than this reputed credit card rate.

---

[4] Section 5.2 (1) Annexure A. NERA Report

Presumably therefore Paypal's potential for 'better protection' refers to other aspects of a transaction. But eBay's own core internal dispute resolution procedures are probably the preferred means of dealing with other types of problems, not a *de facto* payment scheme's procedures.

Therefore it may be appropriate to extend to sellers (consumers of eBay services) some of the 'consumer' style protections normally extended to consumer buyers. And to require participation in the other more mature, perhaps less capricious dispute resolution schemes available for other more traditional payment system participants.

4. Young persons may be more vulnerable.

We are not in a position to explore the actual level and nature of engagement of people under 18 with eBay and PayPal.

However, given their heavy use of the net and propensity to bypass barriers set against them, it may warrant further investigation to consider whether there are particular risks which may be raised for them by the proposal; in particular by greater exposure to phishing spam, above, which they may be less able to detect and ignore.

(Though many young people are reputed to be quite sophisticated in assessing online *bona fides*, this is by no means to be assumed generally, and the normal assumption of less sophistication should apply.)

5. Potential for this case to have a role as an international test case for eBay

EBay is reported to have described the current initiative in Australia as an 'experiment', which if successful will be applied globally.

If this is the case, it has global implications, and all relevant regulators and consumer organisations in other countries potentially affected should have been notified and consulted. This is a further reason for extending the consultation period and substantially improving the consideration of the potential implications.

It is a potential weakness of national laws applied to the Internet that a global operator may in effect seek to 'pick off' specific markets for introduction of a new and controversial practice, and then use its acceptance there as a *de facto* precedent in other locations, initially those less able to resist and later those holding out, who can be characterised as exceptions.

By this means can practices which do not necessarily have global support be introduced incrementally. In the absence of an effective global consumer protection jurisdiction, and because global online practices affect Australian consumers and markets, the ACCC should take whatever steps are available to it to enable consumer and competition interests generally likely to be affected by the outcome of this experiment to provide informed input to its considerations, as they may in effect be a ruling on what becomes a de facto global test case. All interested parties should have some opportunity to offer input, even if Australian interests must have the main attention.

We hope the above comments are all of some value determining how to weigh up the competing claims about net benefit or detriment.

Yours sincerely

David Vaile
Executive Director
Cyberspace Law and Policy Centre

Law Faculty
UNSW Kensington Campus
Sydney NSW 2052 Australia

T: 02 9385 3589
E: d.vaile [at] unsw.edu.au
W: http://www.cyberlawcentre.org/