Inquiry Secretary
House Standing Committee on Communications
House of Representatives,
PO Box 6021,
Parliament House,
Canberra ACT 2600

Dear Sir/Madam

Inquiry into Cyber Crime: Submission

eBay.com.au is Australia's leading online marketplace. Founded in 1995, eBay Inc. connects hundreds of millions of people around the world every day, empowering them to explore new opportunities and innovate together. eBay Inc. does this by providing the internet with platforms of choice for global commerce, payments and communications.

eBay.com.au is pleased to provide comments to the House Standing Committee on Communications' Inquiry into cyber-crime and the effect of cyber-crime on consumers.

Introduction

Consumer trust of the online environment is critical to the survival and success of eBay and eCommerce both in Australia and around the world. As a pioneer of eCommerce with over 5 million Australian visitors a month[1], and 88 million active users globally, eBay understands the threats faced by both consumers and companies operating in the online space.

In traditional (offline) retail , buyers can meet the seller (or the seller's representatives), inspect the goods before purchase, and generally receive those goods immediately upon payment. Online buyers have a different experience and generally will have to pay for items before receiving them and trust that they will arrive. Consequently, unless there are protections in place, online buyers can be more susceptible to fraudulent or bad behaviour by sellers. This may result in:

- items being paid for but not received
- uncertainty over what the total price payable will be
- the received item being significantly different to what was described to the buyer
- misrepresentation as to the true identity and reputation of the seller.

Online buyers are subject to a clear power and information imbalance with sellers, and must rely on the seller's behaviour and (often unilateral) terms of sale when making buying decisions.

In addition, consumers operating in the online space face a range of other criminal threats resulting from merely being online: the theft of their personal financial data, their identity,

[1] eBay is Australia's leading online marketplace with 5 million unique visitors in May 2009 according to Nielsen/NetRatings Netview.

exposure to illegal and inappropriate online content, the misuse of their computing power to attack others, amongst others.

If we are to see eCommerce and broader internet usage continue to grow and to be trusted in Australia it is important that business and government work together, alongside consumers to minimise the threats.

eBay welcomes the opportunity to contribute to the Committee's deliberations on this important matter.

The evolution of online crime

The internet's criminal environment has changed since eBay commenced operations in 1995. As more people have moved to the internet, and with them more money made and traded online, the criminal threat has grown and evolved from a youthful intellectual pursuit, to a cottage industry through to an industrialised, automated series of attacks against the company, the eBay community and indeed all internet users.

Criminals have remained motivated by one thing: to directly access money or to steal personal information which they can later use to get money.

While online crime statistics are patchy at best, there are some credible indicators as to the size and frequency of the problem:

- A recent report by the Australian Institute of Criminology highlighted that businesses victimised in computer security incidents reported only 8% to police and that the cost to business was $649 million in FY2007[2] This figure does not include the cost to consumers that may have stemmed from those incidents.

- While there is no attempt to quantify the loss to Australian consumers through IT security incidents, the AusCert Home Users Security Survey 2008[3] provides interesting data about the level of protection and compromise of the Australian home Internet population. It indicates that only 60% of Australians feel comfortable providing personal information online[4].

- And IT Security company Sophos was recently quoted as saying that 97% of all business email it monitors is spam.[5] While most of that spam is killed off at the network level before it reaches the end user, it highlights how vulnerable the email system is to criminal influences.

It is difficult to quantify what these aggregate criminal activities do to the trust and confidence consumers have in doing business online but it would not be hard to put forth an argument that crime - or fear of crime - online could significantly undermine consumers' online activities.

---

[2] http://www.aic.gov.au/publications/rpp/102/rpp102.pdf
[3] http://www.auscert.org.au/images/AusCERT_Home_Users_Security_Survey_2008.pdf
[4] AusCERT Home User Computer Survey 2008, http://www.auscert.org.au/images/AusCERT_Home_Users_Security_Survey_2008.pdf
[5] The Sunday Telegraph, "How to fake an email and get away with it", 28 June 2009

Fighting online crime

eBay has pursued a multi-pronged approach to reducing the effect of eCrime on the eBay community. It has invested in education as well as the development of systems and the deployment of staff against the problem.

The key indicators of risk consumers should consider when using ecommerce websites

- If a deal seems too good to be true, it probably is.
- Sites/sellers requesting payments for goods or services via means which can't be reversed, offer no protections, and have questionable proof of identity at the receiving end: eg, Western Union or cash in the mail. Consumers also need to be careful of bank to bank transfers as there is no protection offered by banks. Further, evidence suggests that criminals may use legitimate, but compromised bank accounts to receive payments for online crimes

Key advice to consumers

- Apply your offline common sense to your online actions (e.g. you don't use the same key for your home, office and car, so don't use the same password for your different internet accounts).
- Not everyone online is who they say they are - check the reputation of the person you are dealing with (using eBay feedback, for example)
- Type in the URL of the website you want to visit
- Protect your personal information - be wary of how much you put online
- Protect your money - pay online using methods which don't mean you pass your personal financial information to the person you're dealing with, and which also offer protection should something go wrong
- Protect your computer - ensure you have anti-virus and firewall programs running on your computer, make sure they are up to date, and patch the operating system and other software used on the computer

Ongoing consumer education to reduce fraud

eBay believes that all consumers want to get the best deal. As consumers are primarily concerned about finding lower prices online than they might otherwise find offline, there is a risk that they might seek the lowest priced item rather than assessing the safest sale. This is particularly the case for first time buyers who do not necessarily have the experience and knowledge to know what to look out for, or how risky a transaction might actually be. First time buyers who have a bad buyer experience may be deterred from using the internet to purchase goods online in the future. This is ultimately to the detriment of online sellers and eCommerce in Australia.

eBay believes that educating consumers in the area of online safety is a critical tool for reducing online crime, and consumer education has been an ongoing commitment by eBay. Education can have a significant impact. A large portion of the online community

lack the basic skills and experience to operate as safely as they could in the online environment, or (as was recently highlighted in a study published by the Australian Communications and Media Authority[6]) they hold the relevant skills but are not proactive in protecting themselves online.

Education of individuals, and convincing them to improve their behaviour, is increasingly important on the internet as criminal groups have shifted their focus more and more to the consumer end[7]: compromising hundreds or thousands of consumers via an automated attack can be more productive than attempting to steal the same data from a corporate computer system.

eBay is committed to raising awareness about trust and safety issues in transacting online and has a consistent record of educating consumers about how to avoid problematic and fraudulent online transactions. A summary of some of these initiatives is set out below.

eBay.com.au has conducted many education campaigns, including:

- publishing and promoting a "Guide to Safe and Sensible Online Trading" in 2003
- publishing a national eCommerce Safety Guide, the inaugural version of which was officially launched by the federal Attorney-General at the time, The Hon Philip Ruddock MP, in March 2005;
- publishing trust and safety advertorials in popular womens' magazines, newspapers and other publications in 2005;
- conducting the "Everyone's Doing It" advertising campaign in January 2006 which explained the benefits of the PayPal Buyer Protection policy;
- publishing a white paper on phishing in March 2006;
- publishing a national "Web Smart" paperback guide in June 2006;
- conducting an education campaign on phishing in September 2007;
- conducting a trust and safety campaign called "The Real Bad Guys" in 2007 to educate consumers about various internet threats;
- sending regular direct emails to the eBay.com.au community explaining ways in which consumers can protect themselves online and providing information about the dangers of different types of identity fraud.

eBay.com.au provides extensive onsite education, including:

- providing onsite information via its Security Centre (which is regularly reviewed and updated) and other help pages, as well as links to third party resources such as the ACCC;
- serving interstitial (interim/pop-up) pages during the bidding and buying (and selling) flows on eBay.com.au to educate members about safe trading, items that might be prohibited, transaction risks, etc;
- serving interstitial (interim/pop-up) education and warnings following product recalls or other one-off events

[6] Australia in the Digital Economy, Report 1: Trust and confidence, March 2009, see particularly sections 5 & 6 http://www.acma.gov.au/webwr/aba/about/recruitment/trust_and_confidence_aust_in_digital_economy.pdf

[7] The shift first started to occur at a large scale with phishing, which involved spam emails and fake websites. Other automated attacks using malicious code are also launched on a regular basis against internet users.

- providing trust and safety education messaging to eBay.com.au members upon signing-in to the eBay.com.au website, such as reminding members to update their password;
- serving trust and safety related messaging through onsite banners and onsite advertising placements;
- prohibiting the use of, and educating consumers about the shortcomings of using, certain payment methods online such as Western Union, where consumers may transfer money to people they do not already know or trust. (Regulators and law enforcement including the various Australian state police forces and the ACCC have fact sheets highlighting the problems caused by money transfer scams and providing golden ruled to help beat the scammers.)

eBay.com.au has actively participated in a number of government and private sector partnerships and initiatives, including:

- eBay's unique partnership with the Queensland Police to establish a Police website in 2006 to manage the reporting of online auction fraud, which allowed members of the public to prepare their own statements, participate in eBay's online dispute resolution process, and report directly to the police jurisdiction where the offender lives, in order to save police thousands of hours of police investigations and reduce the need for police intervention in problematic transactions;
- the Federal Government's eSecurity Awareness Week hosted by the Minister for Broadband, Communications and the Digital Economy, where eBay was a member of the Steering Group, and sent direct emails to several million eBay community members raising awareness of the Government's message about safer online practices;
- the Australasian Consumer Fraud Taskforce, which is an independent body chaired by the ACCC that runs the annual 'Scamwatch' program distributing educational materials to consumers;
- in conjunction with CrimeStoppers and Western Union, launching the Security Awareness and Fraud Education Program (SAFE) to educate the community on different types of fraud and advise consumers on the precautions they should take when transacting with people they do not know, such as advising buyers to not use Western Union to make payment to sellers they do not know for items purchased on eBay.com.au;
- conducting regular outreach programs with law enforcement and government agencies, such as the state Offices of Fair Trading (there have been approximately 5000 programs conducted in the last seven years) and
- hosting numerous police conferences and education workshops each year.

Systems, policies & staff

While eBay will continue to educate consumers about safer online practices, eBay knows from first hand experience that education alone is not sufficient in reducing the incidence of online fraud and disputes. In addition to some buyers' decisions to take a risk and believe that "bad things won't happen to me", buyers in the online retail environment suffer from "information asymmetry", in being less informed about their purchase because they cannot physically inspect the goods, unlike offline consumers.

The risks of online fraud are further demonstrated by a recent Harvard University study in relation to "phishing" and "spoofing". What the study shows is that online fraud poses a

threat to even alert and experienced online consumers. In its concluding section, the authors of the study relevantly state[8]:

"This study illustrates that even in the best case scenario, when users expect spoofs to be present and are motivated to discover them, many users cannot distinguish a legitimate website from a spoofed website. In our study, the best phishing site was able to fool more than 90% of participants…

"Furthermore, the indicators of trust presented by the browser are trivial to spoof. By using very simple spoofing attacks, such as copying images of browser chrome or the SSL indicators in the address bar or status bar, we were able to fool even our most careful and knowledgeable users…

"Participants proved vulnerable across the board to phishing attacks. In our study, neither education, age, sex, previous experience, nor hours of computer use showed a statistically significant correlation with vulnerability to phishing." (emphasis added).

What these results clearly show is the need for consumers to receive more than just education to combat online fraud as education and experience alone have been proven to be insufficient tools for fraud detection.

Very early in the company's history eBay recognised that it needed to invest in developing rules of behaviour, systems and technologies as well as staff to help keep the site safe. To this end eBay has invested many millions of dollars and committed significant staff resources to addressing the criminal misuse of eBay systems.

One of the most significant hurdles faced in the online environment is that of identity and reputation: how do you know who you are dealing with, and how do you know you can trust them? Just as in the offline world, online there are criminals and those who take shortcuts and abuse systems. But online many of us lack the experience - and in some cases the skills - to navigate as safely as we should.

eBay recognises that the issue of online reputation is critical. If a buyer and seller see how the other person acted previously, it is a good predictor of how they might behave the next time.. And so the "feedback" system was created. With over six billion feedback comments left since inception, the eBay feedback system - which has been modified over the years - has enabled millions of people to develop a trusted identity (and corresponding reputation), and to interact and conduct commerce over the internet totaling hundreds of billions of dollars.

The eBay feedback system reflects the 5 core values of the company:

1. We believe people are basically good

2. We believe everyone has something to contribute

3. We believe that an honest, open environment can bring out the best in people

4. We recognise and respect everyone as a unique individual

5. We encourage you to treat others the way that you want to be treated

---

[8] people.seas.harvard.edu/~rachna/papers/why_**phishing**_works.pdf

Early in the company's development eBay also realised that the eBay community cared greatly for their reputations and were determined to help keep people honest. Still today eBay operates the world's largest neighbourhood watch system, where eBay members are encouraged to report illegal or improper items being sold on the site. Millions of eyeballs scanning eBay dramatically reduce the likelihood of criminals operating in plain sight. Online criminals are similar to offline criminals in that regard.

Hand in glove with community reporting, eBay began to develop internal systems to monitor the site, and employ operations staff to act on reports from the detection systems and the eBay community: just because most people were "basically good", did not mean that all of them were.

While it is these internal systems and rules we will mainly focus on in this submission, it is important to remember the strong community involvement and the almost unshakeable robustness of the feedback reputation system.

Preventing fraudulent accounts

While eBay endeavours to maintain an open door to legitimate customers with minimal barriers to entry (just as offline stores), it also needs to make it hard for criminals to register accounts (particularly with the potential to sell items which may not exist).

One of its priority areas in fraud minimisation has been to stop fraudsters from being able to operate on the site in the first place. Using sophisticated risk modeling, as well as tying accounts to offline identifiers such as fixed landline telephone numbers has allowed eBay to know sellers better and made it harder for fraudsters to open new accounts. In addition, requiring sellers to identify and show control over a bank account (using the PayPal Verified process) through a series of random deposits to those accounts, makes registering much more frustrating - and risky - for criminals.

The eBay community has been the subject of criminal attack in the form of phishing emails (which purport to be from the company and urge a person to click into a fake eBay website and enter passwords and other valuable information). It is logical that eBay has been a widely misused brand: with hundreds of millions of members worldwide, all of whom are online, and expecting to communicate with the company and each other via email. As such, eBay has heavily invested in anti-phishing efforts, including alliances with Yahoo!, Google and others to block phishing e-mails before they arrive in users' inboxes.

The eBay community has a number of ways to check if a message is genuine, these include:

- Checking messages in My eBay – If an email affecting the status of an eBay account is legitimate, it will always appear in the My Messages section of My eBay. If it isn't in My Messages and it's to do with an account, it's likely to be fake.

- Downloading the eBay Toolbar – the free eBay toolbar has Account Guard which turns green when a person is on a genuine eBay or PayPal site and red when s/he is on a potentially fraudulent site.

- Reporting suspicious emails – eBay and PayPal have specific addresses for users to report and send any suspicious emails to in order to verify its authenticity. These email addresses are spoof@ebay.com.au and spoof@paypal.com.au. It is

recommended that the entire suspicious email is forwarded to one of these addresses and then deleted immediately from the user's system.

eBay also protects the eBay community by deploying other technologies which note which computers eBay members typically use to conduct their buying and selling activity allows the company to identify potentially riskier transactions where the buyer or seller has logged in using a different computer (which may be because a criminal has stolen their password). In this case eBay may make an automated call to the phone number the eBay member registered to confirm it is really them, or ask further identity questions of the seller.

Reducing fraud visibility

eBay knows that no process can prevent all criminals from registering on the site with the intention of defrauding others. So, it has pursued a parallel policy of reducing the visibility of fraudulent items, that way, if fraudsters manage to get hold of an account, systems make it unlikely that their fraudulent listings will become visible to the Community.

In April 2007 the company announced that items most favoured by fraudsters would not be visible in search for a number of hours. During those few hours, fraud detection algorithms and investigators in the company's 2,000-plus Trust & Safety team work to stop fraudsters and their listings before they ever become visible to the community. By July 2008 fraud visibility dropped by over 80%.

Community reporting of visible (possibly missed) fraudulent listings helps the company to continually improve detection algorithms.

This same system is used to monitor eBay for listings which are in breach of product safety or regulations (such as pharmaceuticals). Teams of operations staff work 24/7 to review and action listings which may fall into these categories. In fact, eBay has seen instances where consumers have received greater protection because they have purchased online rather than in an offline store, for example, in November 2007 the Bindeez childrens' toy was recalled due to dangerous chemical reactions when children placed the beads from the toy in their mouths. eBay was able to immediately remove all Bindeez listings, place filters to prevent new listings, and also to provide details of previous buyers and sellers of that product to consumer safety regulators so that they could advise them of the danger. Such actions would not be possible in the offline environment due to the record-keeping of those institutions.

In 2008, eBay expanded the use of anonymous bidder IDs to all auction listings which protected under-bidders and winners from fake (fraudulent) Second Chance Offer requests and other malicious spoof email. Fraudsters used to gather bid history information from the site to identify User IDs of unsuccessful bidders and combine it with information from other places (like the item page) to send authentic looking emails which appeared to offer the same or similar items for sale.

Because a significant number of eBay members have registered an email address that is very close or identical to their eBay User ID, fraudsters send spam emails to bidders using the User ID along with several of the most common domain names (eg userid@hotmail.com.au, userid@yahoo.com.au, userid@gmail.com, etc). Some of those emails reached their target.

Upon receiving these emails unsuccessful bidders may have thought they were dealing with the legitimate original seller, and agreed to send funds in exchange for the item.

As a result of the use of anonymous bidder IDs, fake Second Chance Offer volume declined by over 90%.

Fraudsters can also attempt to use e-mail to coax buyers into unsafe, off-eBay transactions, even before the auction closes. To counter this, eBay has continued to introduce safer member-to-member email via anonymous email forwarding, which keeps pre-sale communications safe on eBay and keeps the buyers' e-mail address anonymous and protected.

Ensuring safer transactions.

For eBay.com.au buyers, PayPal Buyer Protection may protect the full purchase price and original shipping costs of eligible purchases, up to a total of $20,000.

All PayPal customers also continue to be 100% protected against unauthorised payments sent from their PayPal accounts.

For eligible eBay sellers, PayPal also offers protection against payment reversals due to unauthorised payments (for example, payments made with stolen credit cards) and buyers who claim they haven't received items they've bought as part of the PayPal service offering.

eBay requires sellers to accept payment via PayPal on most listings on eBay.com.au, however sellers may express a preference for any permitted payment method. Buyers may choose to pay by any of the methods accepted by the seller. This policy enhances consumer protection for eBay.com.au purchases in a number of ways, including the following:

- when making or receiving payments via PayPal, neither trading partner has access to the other's sensitive financial information. This greatly reduces the chances of identity theft and financial fraud and greatly enhances consumer confidence for trading online;

- as eBay and PayPal are related bodies corporate, a 'closed loop' transaction is created when buyers make payment via PayPal for items purchased on ebay.com.au, allowing eBay and/or PayPal to monitor and help prevent fraud throughout the entire transaction process and on a real-time basis;

- furthermore, as related bodies corporate, eBay and PayPal are in a unique position to share sensitive transactional and financial information regarding their members to assist in detecting fraud, and intervene in eBay.com.au transactions for consumer protection purposes; and

- PayPal is able to place temporary holds or freezes on funds for risky transactions, can reverse funds to buyers, and may make payment to buyers under its Buyer Protection policy (up to $20,000 per transaction) in the event that an item does not arrive or is significantly different to what was described by the seller.

In comparison, where bank deposit is used as the preferred payment method on

eBay.com.au and the transaction results in a buyer not receiving the item they have paid for, the buyer has no guarantee that their money will be refunded. Banks declare that they are not obliged to track the funds, or reverse the funds in the case of error (such as buyers typing in the wrong bank account details), fraud, or simply non-receipt of an item.

For example, Westpac states in its *Internet Banking and BPAY Product Disclosure Statement* that: "Westpac cannot reverse transactions you make in error, either to Westpac or non-Westpac accounts. Should an amount sent by you in error not be returned automatically by the receiving financial institution, it may not be recoverable at all."

Since PayPal is a related body corporate of eBay and is therefore integrated into the eBay Checkout system, buyers do not face the same problems and risks of incorrectly typing in the bank details of the seller. [9]

Further, internet banking transfers are not subject to the transaction-level hold protections provided by PayPal. Failure to provide such systems creates a great problem of fraudulent transactions happening in the first place, as demonstrated by the fact that the dispute rate for transactions on eBay paid for using this payment method is almost 4 times higher than that for PayPal.[10]

The weaknesses in the direct deposit system as outlined above are not commonly known by consumers as the major banks clearly will not advertise or promote this consumer disadvantage.

Conclusion

The cyber crime inquiry provides a great opportunity for the Government and industry to work together to educate the community and build systems to help keep consumers safer online and to build trust in eCommerce.

To assist online consumers who pay through direct deposit, eBay would especially encourage those in the financial services sector who do not provide buyer or seller protection to do so, and, to develop and better use systems to track funds, or reverse funds in the case of error. These systems and protections provide greater security and peace of mind for online consumers. This is beneficial to both the consumer and eCommerce in general.

eBay has worked closely with the Federal Government in its efforts to educate the community through eSecurity Awareness Week hosted by the Minister for Broadband, Communications and the Digital Economy. eBay would welcome the opportunity to work with the Government on further eSecurity education intitiatives.

---

9 http://www.westpac.com.au/manage/pdf.nsf/0228F1395778BD49CA2573240082FDC7/$File/IB_PDS_new.pdf?OpenElement

10 eBay.com.au 2007 data