



Ms Jane Hearn
Secretary
Standing Committee of Communications
House of Representatives
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Ms Hearn

PayPal Australia Submission for Inquiry into Cyber Crime

Founded in 1998, PayPal Inc was acquired by eBay Inc in 2002. Globally, PayPal provides internet users with a faster, safer and easier way to pay and get paid online. Available in 190 markets and 19 currencies¹, PayPal is a global leader of online payment solutions, with over 70 million active accounts worldwide.²

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

Introduction

The Federal Government is to be commended for its many initiatives designed to increase access to online services by all Australians. The Government's National Broadband Network will provide more people with access to the internet and with faster internet speeds. Consequently, internet use is likely to increase. It is therefore essential that the community is provided with the skills and thus the confidence to use the internet safely and effectively.

In the 2008 eBusiness Sensis Report, businesses noted that the community's concern about computer hacking was a barrier to eCommerce.³ This suggests a general lack of confidence in online security.

eCommerce can provide a wide range of benefits to both consumers and merchants. For consumers, online retail provides a broader selection of goods at generally lower prices. Selling goods online provides business opportunities for people in remote areas and allows goods to be seen by literally anyone with internet access! To ensure Australia realises the potential benefit of the internet and the digital economy, consumers need to trust the online environment. Key to developing trust in eCommerce is the provision of a safe online payment method. PayPal was founded on these principles.

¹ Chinese Renminbi can only be used within mainland China

² Active accounts are those that have had activity in the past 12 months

³ Sensis, *e-Business Report: the Online Experience of Small and Medium Enterprises*, p.30 (June 2008)

The online and offline markets are significantly different. The online payments market posing unique problems to eCommerce. 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 the goods will arrive. Consequently, unless there are protections in place, online buyers can be more susceptible to fraudulent or bad behaviour. For example:

- items may be paid for but not received
- the buyer may be uncertain about what the total price payable will be
- the received item might be significantly different to what was described to the buyer
- the seller can misrepresent their true identity and reputation.

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

Conversely, an online seller is more susceptible to credit card fraud, as the seller does not have the opportunity to inspect the physical card. Also a fraudulent buyer could falsely claim that the purchased goods or services were not as described or never received.

Consumers (both buyers and sellers) operating in the online space face a range of other criminal threats that result from merely being online: the theft of their personal financial data, theft of their identity, exposure to illegal and inappropriate online content, the misuse of their computing power to attack others, amongst others.

PayPal was developed specifically to address the unique needs of the online environment and the peculiarities of the eCommerce market. PayPal's closed loop system⁴ offers a safer means of transacting online by leveraging the existing payments infrastructure.

PayPal provides consumers with the ability to pay for items using a credit or debit card, bank account or PayPal balance. PayPal is safer for consumers as during a transaction financial details are safely stored on PayPal's servers and never shared between buyers and sellers. Sellers can withdraw the money to their bank account or keep the funds in their PayPal account for online purchases.

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

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

Cyber crime

The internet's criminal environment has changed dramatically over the years. Online crime used to be the domain of hackers who were technically savvy and concentrated mainly on corporate and government networks. Today, as more people use the internet

⁴ PayPal oversees the entire transaction between the buyer and seller. In this manner PayPal operates as a closed-loop payment system with visibility into both the buyer and seller sides of the transaction, whilst the information belonging to one entity is generally not divulged to the other.

for social and retail purposes, online crime concentrates on exploiting individual and network vulnerabilities for financial gain or politically motivated attacks.

Online crime is no longer carried out by one or two individuals. There are now organised criminal groups online who seek to exploit any and all computers connected to the internet through automated attacks. These criminal groups have established bot networks (botnets)⁵ at locations all around the world to send spam, carry out phishing attacks and apply keylogging applications⁶ - amongst other things. Their aim is to make a profit, either through stealing personal identity information or financial information (often sent when making an online purchase) which can then be used or sold to others.

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 FY2007⁷. This figure does not include the cost to consumers that may have stemmed from those incidents.

The Unisys Security Index⁸ reports that 55% of Australians are very or extremely concerned about other people obtaining credit card / debit card details and 54% of Australians are very or extremely concerned about unauthorised access to / or misuse of personal information. This is not surprising when the Australian Bureau of Statistics has researched the number of consumers victimised through identity theft and scams and estimates that nearly 500,000 Australians were victims of identity fraud in the 12 months prior to the survey.⁹

While it is not possible to calculate the exact impact criminal activity has online it is clear that it would have an impact which would undermine both eCommerce and consumer confidence. It is critical that Government and industry work together to build and maintain consumer and business confidence in online transactions.

PayPal

PayPal operates an online payment service that allows its members to make financial transactions with one another over the internet or mobile phone without providing the other party with private financial information, such as bank account or credit card details. For recipients of funds, PayPal offers (amongst other services) a service, whereby it will process credit and debit card transactions without the need for the recipient to have a merchant facility with a financial institution.

PayPal can be used to facilitate transactions between individuals for most online transactions. Customers must in all cases use their linked bank account, debit or credit card or stored (PayPal) balance to fund transactions, with PayPal forming a closed-loop conduit through which the transactions take place.

In the case of credit or debit card transactions, PayPal acts as the merchant of record, thereby avoiding the need for sellers to obtain a merchant facility from a financial institution. Customers are unable to use PayPal without first associating a funding source

⁵ The word BOTNET is short for the combination of robot and network. The term often applies to groups of computer systems that have had malicious software installed by worms, Trojan horses or other malicious software that allows the botnet's originator to control the group remotely.

⁶ A software program that records the keystrokes entered by a user on a particular computer.

⁷ <http://www.aic.gov.au/publications/rpp/102/rpp102.pdf>

⁸ <http://www.unisyssecurityindex.com/australia/>

⁹ Australian Bureau of Statistics, *Personal Fraud Report 2007* (June 2008)

from a traditional financial institution in the form of a bank account, debit or credit card or where they have received funds which are in the form of a stored balance.

Where a PayPal account is linked to a bank account, the account holder must demonstrate that he or she controls that bank account before it can be used to fund any payment. In the case of credit or debit cards, PayPal may undertake security checks on the card and, in some instances verification is undertaken by PayPal independently.

There are a number of different account types that a PayPal member may open, namely Personal, Premier or Business accounts. The fees imposed on members differ depending on the type of payment made (or received). Fees apply most commonly to the receipt of funds by sellers, although senders of payments that require a currency conversion will pay an exchange rate that includes a spread for PayPal. To that end PayPal is considered to be generally free for senders of payments/buyers.

When a PayPal member sends funds to another PayPal member, notification of the amount will immediately appear in the recipient's PayPal account. However, for bank-funded payments, depending upon the circumstances surrounding the payment, access to these funds may be withheld for a short period for risk mitigation purposes. Where a buyer has a back up funding source, such as a credit or debit card, then PayPal will make the payment instantly. PayPal itself, and not the merchant, assumes the risk of insufficient funds by the buyer.

Where a problem arises with a payment, PayPal has the power to reverse transactions, although it will try a number of alternatives before doing this. This is an important safety mechanism to avoid disputes.

PayPal's closed loop system is illustrated in the following diagram:



PayPal aims to promote online consumer confidence through two key measures: eSecurity and privacy. Together they are intended to combat the biggest risks faced by consumers.

eSecurity

Ensuring safer transactions

As stated above, PayPal can be used to facilitate transactions between individuals for most online transactions where customers use a linked bank account, debit or credit card or a stored balance to fund transactions.

PayPal oversees the entire transaction between the buyer and seller, whilst the financial information belonging to one entity is not divulged to the other. In this manner PayPal operates as a closed-loop payment system with visibility into both the buyer and seller sides of the transaction.

If either a buyer or a seller raises a complaint regarding the transaction (for example, if a seller complains about non-receipt of funds or a buyer complains about the condition of goods received), PayPal can and does act as an intermediary in resolving the dispute. PayPal's Online Dispute Resolution process has yielded excellent results.

PayPal's Unique Customer Protections

PayPal's closed-loop nature and ability to see both sides of an online transaction means that it is far easier for PayPal to protect its members from fraud and significant losses.

For PayPal members who purchase eligible items on eBay, PayPal offers additional buyer protection where an eligible item is not received or is "significantly not as described". Under PayPal's Buyer Protection Policy members that purchase eligible items on eBay Australia can currently be protected for up to \$20,000 for any purchase (excluding certain categories, such as intangible items).

Even when PayPal Buyer Protection is not available, PayPal's Buyer Complaint Policy is available. In that case, if and when the buyer files a dispute against the seller, PayPal will put a hold on funds in the seller's account in the amount of the transaction, pending resolution of the dispute, but does not guarantee a reversal of the transaction.

PayPal also offers security benefits for sellers. In 2007, eBay.com.au sellers who accepted PayPal were about half as likely to experience an unpaid item by a buyer than sellers who did not accept PayPal.¹⁰ Nevertheless, in an Australian first, PayPal Australia has also introduced additional protection for eligible sellers through its unique Seller Protection Policy, at no additional cost to sellers.

Under the Seller Protection Policy, PayPal will not reverse transactions for eligible eBay sellers for unauthorised payments from buyers' PayPal accounts or stolen credit cards, or situations where a buyer claims "item not received" if the seller can provide proof of shipment of the item through an approved postage service and other information, as required by PayPal. In this event, sellers will be entitled to retain the disputed funds and in these cases PayPal absorbs any losses that would otherwise be borne by the seller.

The risks of online fraud are demonstrated by a recent Harvard University study about "phishing" and "spoofing". The study shows that online fraud poses a threat to even alert and experienced online consumers. In its concluding section, the authors of the study

¹⁰ Research conducted by eBay on eBay.com.au related transactions, 2007.

state¹¹:

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...

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.

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.

PayPal's fraud and risk monitoring

PayPal recognises that online security must be an essential part of every online business, given the unique risks that the online environment poses. For this reason, PayPal helps protect merchants by providing a payment system that comes with built-in, world-class anti-fraud screening to minimise transaction loss (at no additional cost to the customer). As the merchant of record, PayPal also represents merchants where there are disputed chargebacks.

PayPal's risk analysis is a combination of factors unique to PayPal which operate in real-time to prevent fraud and money laundering in the system. PayPal's closed-loop structure means PayPal is in a unique position of having access to both the sender's and the receiver's accounts to aid in assessing the risk associated with a transaction.

All of PayPal's protection policies and risk mitigation procedures, discussed above, have led to the public recognition of PayPal by eminent international authorities at the Financial Action Task Force¹² ("FATF"). FATF has deemed PayPal's business model and service as the benchmark for new online payment methods when it comes to safety and security online.¹³

In their March 2008 Consumer Confidence in Online Shopping study, market research agency Stokes Mischewski found that the majority of Australian online shoppers believe PayPal is the safest method for online payments: 59% of Australian internet shoppers consider PayPal to be the safest online payment method over bank deposit (14%), credit cards (11%) and money order/cheque (4%).¹⁴

¹¹ www.people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf

¹² The Financial Action Task Force is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing.

¹³ "Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems" June 2008, located at:

<http://www.fatf-gafi.org/dataoecd/57/21/40997818.pdf>

¹⁴ Stokes Mischewski *Consumer Confidence in Online Shopping* March 2008. The study involved an online survey of 650 Australians who use the internet more than once a week. The age, gender, state and region profile of the sample was matched to ABS data on the demographic profile of regular internet users ages 18 years and over. Given an online panel is likely to over-represent online shoppers, quotas ensured the proportion of online shoppers (vs. online consumers who do not shop online) in the sample matched AC Nielsen data on the proportion of online shoppers in the Australian online population.

All the above leads to the fact that PayPal globally has fraud loss rates, which we believe to be amongst the lowest in the online world. Furthermore this loss rate is trending down.¹⁵

Globally, PayPal deploys the following programs:

- low value based limitations on sending money and withdrawing money which triggers our own specially devised verification procedures;
- the use of real-time transaction monitoring and case management technology for money-laundering and terrorist financing (AML/CTF) red flags and risk;
- enhanced customer due-diligence processes where a specific high-risk activity is detected (such as sale of high value items such as jewellery, and accounts claiming to represent charitable organisations);
- screening of all customers against Government watch lists;
- account registration controls; and
- controls that require a customer to verify a financial instrument when adding it as a funding source to a PayPal account. For example, if the customer links a specified bank account to their PayPal account, then before the PayPal account is verified, PayPal will send two random deposit amounts to the bank account. Once these deposits are received the customer can verify their control of the account by advising PayPal of the two amounts. This proves access and control over the linked bank account and is referred to as the “random deposit process”.

These programs are enhanced by the structure of the PayPal service, which is built on top of the existing banking infrastructure, so all incoming funds come from bank accounts or payment cards which have already been subject to the appropriate collection and verification protocols by the respective institution and by the fact that the PayPal service is a closed-loop system.

These processes help make PayPal a leader in online payments safety and security.

In summary, PayPal delivers one of the most powerful online risk management systems in the world for merchants (and buyers) and is recognised as a leader in privacy and identity protection.

Education

PayPal combats online risks through the use of its security centre.¹⁶ The centre provides information on identity theft, phishing, spoof websites, security tips, security tools and useful links to sites that provide information on online safety best practices from around the world.

The centre can be used as a stand alone source of safety information, or can be used in conjunction with Government sites, which it endeavours to reference and provide links for. PayPal firmly believes the better educated a consumer is about transacting online the more confident they will feel.

¹⁵ PayPal global, internal research

¹⁶ https://www.paypal.com/au/cgi-bin/webscr?cmd=_security-center-outside

PayPal regularly reviews and updates its education and information measures as well as other cyber safety resources which are designed to meet the needs of consumers wishing to buy and sell online.

PayPal provides a number of key messages to consumers to try and raise eSecurity awareness and provide education.

Key advice to consumers includes:

- Protect your money - pay online using methods which do not pass your personal financial information to the person you are dealing with, and which also offer protection should something go wrong
- Apply your offline common sense to your online actions (for example, 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)
- Protect your personal information - be wary of how much you put online
- Type in the URL of the website you want to visit, don't click on a link in an email
- Protect your computer - ensure you have anti-virus and firewall programs that are up to date, and patch the operating system and other software used on the computer with regular updates provided by the vendor.

PayPal 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 PayPal. 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 Authority¹⁷) they hold the relevant skills but are not proactive in protecting themselves online.

Educating individuals, and convincing them to improve their behaviour is increasingly important on the internet as criminal groups have shifted their focus to defrauding consumers.¹⁸ The criminals can now target hundreds or thousands of consumers via an automated attack, which can be more productive than attempting to steal the same data from a corporate computer system.

PayPal 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.

Privacy

¹⁷ 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

¹⁸ 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.

PayPal is an online payment service that allows its members to make financial transactions with one another over the internet and mobile phones without providing the other party with financial information, such as bank account or credit card details. To that end PayPal is founded on privacy and maintaining the confidentiality of a user's personal data and financial details.

As eBay and PayPal are related bodies corporate, a 'closed loop' transaction is also created when buyers make payment via PayPal for items purchased on eBay, 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 relevant information regarding their members to assist in detecting fraud, and intervene in eBay transactions for consumer protection purposes.

Conclusion

The cyber crime inquiry provides a valuable 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.

The internet is now the most common way for Australians to make contact with government.¹⁹ As part of its Innovation Agenda, the Australian Government has committed to increase the use of Information and Communication Technologies (ICTs) to improve its service delivery. Equally, the Government should ensure it provides the safest way for consumers to make payment as part of this process. The government at a Federal, State and Local level can contribute to consumer confidence by providing a safe online payment method, such as PayPal, to consumers who choose the government's online delivery service methods for paying their bills, rates or taxes.

Safe and secure means of payment online are critical to the growth of eCommerce in Australia, where online fraud and security are increasingly significant issues. PayPal provides a safer and more secure means of transacting online and this is evidenced by industry-leading low fraud rates, when compared to other payment types.

PayPal 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. PayPal would welcome the opportunity to work with the Government on further eSecurity initiatives.

¹⁹ Department of Finance and Deregulation, *Interacting with Government: Australians' use and satisfaction with e-government services* p1 &2 (2008)