PayPal is pleased to submit the following comments on the Preliminary Report of the Whois Task Force. We oppose adoption of the “OPOC proposal” contained in Appendix A of this report.

PayPal, an eBay Company, enables any individual or business with an email address to securely, easily and quickly send and receive payments online. PayPal is a global leader in online payment solutions with 100 million account members worldwide, and is available in 103 countries and regions around the world.

Unfortunately, the PayPal service is also among the most popular targets of phishing schemes and similar online frauds. That is why we invest significant resources in anti-phishing research and investigations.

Typically a phishing scheme involves a counterfeit website that includes the brand name of the target, to which innocent consumers are lured or directed by spam e-mails and other techniques. The victims are then tricked into divulging financial data, passwords, and other confidential information. The problem is growing. The Anti-Phishing Working Group reports that, in October 2005, there were 4367 identified unique phishing URLs. That number soared to 37,444 in October 2006, a 757% increase in one year.

While phishing generally involves criminal activity, the private sector plays a leading role in the detection, investigation and resolution of phishing incidents. One reason for this, besides the limited resources of law enforcement agencies, is that speed is critical in responding to these attacks. The damage inflicted on consumers in terms of identity theft, fraud and other harms increases dramatically every hour that a spoof site remains undetected and unchallenged.

PayPal conducts a Whois lookup in virtually every phishing investigation it undertakes. This provides us with instantaneous access to information about the domain name associated with a particular spoofed site, including information on who has registered it and who is listed as the administrative and technical contact for the registrant. Even if this data is false or incomplete, which some of it often is, it provides clues and leads to experienced investigators as they seek to shut down the site and to identify the perpetrator of the fraud.

This is why PayPal is very concerned about the “OPOC proposal” in the Whois Task Force report. Under this proposal, information on the domain name registrant (other than name and country/state/province) and about administrative and technical contacts would no longer be available to us via Whois. Deleting this information from Whois will inevitably make our response to phishing incidents slower than it is today. Because the OPOC proposal does not provide any alternative procedure for obtaining this information, it would degrade an important tool that we use on a daily basis to combat phishing, protect the privacy and security of innocent consumers, and help to build public confidence in the Internet and in e-commerce.

Instead of the Whois data that we now use (and that has always been available, almost instantaneously, to anti-phishing investigators), the proposal provides for display of the contact information of an “operational point of contact.” If this contact were a responsible party with the capability of shutting down the spoof site, this could be valuable information to have accessible. However, we very much doubt that such a person would ever be designated as the OPOC by a registrant involved in phishing activities. Information on the OPOC is unlikely to be useful in combating phishing.

Of course, PayPal uses Whois data for many other purposes besides responding to phishing, including legal and regulatory compliance and policing our valuable trademarks against infringement. Because public access to Whois data has been a feature of this service since it began (and Whois long predates PayPal), the availability of this information resource is integrated into many of our business processes. If this long-standing feature of Whois is to be discarded or restricted by ICANN (which PayPal would not support), we urge ICANN to first put into place a reliable mechanism by which PayPal and other entities with a legitimate need for contact data can speedily obtain it. This mechanism would have to be available, at a minimum, for any domain name registered in any generic Top Level Domain, by any registrar; and it would need to be accessible, not only to PayPal, but also to the literally thousands of other online businesses, trademark owners, non-profit institutions, law enforcement agencies, and other entities with a legitimate need for immediate access to this data.

PayPal thanks ICANN for considering our comments on this report.

John Muller

General Counsel

PayPal, Inc.