## Senate Estimates 4 June 2013 – Section 313

## Spoken Opening

- Thank you Chairman. I am pleased to appear before the Committee this evening.
- I want to highlight one crucial issue – ASIC's actions to disrupt and block websites run by criminal syndicates engaged in investment scams.
- These criminal syndicates are often based outside of Australia. They have taken many millions of dollars from thousands of Australians, often with devastating consequences.
- One of ASIC's most effective tools to disrupt the websites of these criminal operators is through requesting telecom providers to block access to scam websites under s313 of the Telecommunications Act. Over the last 12 months, **we have used this 10 times.** We are generally quite public about this type of action as we want consumers and the media to understand the risks and the sites we are targeting. In most cases we issue media releases. We have found that quick action in this way can minimise losses.
- Recently, in targeting of a scam investment website, we received information that another site (Melbourne Free University) that shared the same internet address was also blocked. ASIC was unaware the IP address was also shared by other websites. We took immediate action to rectify the situation.
- This was the first time we became aware that we had blocked other sites. We have only heard of the one expression of concern. We have had no indications from telecommunications carriers that this has been a source of complaints. We have received no indications from other regulators, such as the Australian Communications and Media Authority, that there have been any complaints or concerns raised about ASIC's actions.
- Nonetheless, ASIC obviously does not want to impact legitimate sites. We are only interested in disrupting illegal, fraudulent sites. So, we have reviewed the other occasions on which we used this power. I want to briefly tell what we found and set out how we will undertake this activity in the future.

- In the most recent action access to around 1200 websites was temporarily blocked as they shared the same IP address.
- In one other instance in March this year, an IP address we blocked hosted a very large number of sites, around 250,000, of which the vast majority (in excess of 99.6%), appear to contain no substantive content. In this instance we believe that less than 1000 active sites (less than 0.4%) may have been temporarily affected. None of these are .au sites. There are various reasons why such a large number of sites with no substantive content may use the same address, such as through a 'domain for sale' operation.
- On the other 8 occasions only the targeted criminal site, or the targeted site and a very small number of other sites have been affected.
- I repeat we have received no complaints or expressions of concern beyond the Melbourne Free University matter I referred to earlier.

**Next Steps**

- We are consulting with relevant government agencies, AFP cybercrime unit and other law enforcement agencies and the Telecommunications Carriers to determine how we can best disrupt websites that are part of criminal operations without impacting on legitimate sites.
- We are examining:
    - How we can ensure that only the specific URL / Domain Name of the criminal site is targeted, and how s313 may assist in this context;
    - What steps we can take to get voluntary compliance by domain registries to suspend or take down websites, although this is not always straightforward for overseas based operations; and
    - Whether we can have a pop-up page indicating why access has been blocked and to whom queries can be made.
- We are also making a commitment that we will publicly report on our use of s313 on an annual basis. After all, ASIC is seeking to be a public as possible in our attempts to stop Australians being tricked into handing their hard earned money to offshore criminal syndicates.