ASIC
Australian Securities & Investments Commission

GREG TANZER
Commissioner

Level 5, 100 Market Street, Sydney
GPO Box 9827 Sydney NSW 2001
DX 653 Sydney

Telephone: + 61 2 9911 2277
Facsimile: +61 2 9911 2010

Our Reference: CCU-15\0157

20 April 2015

Mr Stuart Woodley
Committee Secretary
Standing Committee on Infrastructure and Communications
Parliament of Australia
House of Representatives
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Mr Woodley

I refer to your letter of 12 March 2015 seeking further information regarding ASIC's use of s.313.(3) of the Telecommunications Act 1997.

A number of the matters raised in your letter were the subject of our written submission to the Committee and our oral testimony before the Committee.

ASIC's further responses to your questions adopt the numbering from your letter.

1. As the financial services regulator, ASIC has a responsibility for investor and consumer protection in financial services. This includes playing a leading role in combatting investment fraud targeting Australian investors. Such fraud includes 'cold calling' investment fraud—colloquially known as 'boiler room' fraud.

   Typically in these frauds the perpetrators cold call their targets and use high-pressure sale techniques to encourage them to transfer money into sham or worthless investments. They use fraudulent websites to back up their claims, lure potential investors to contact them and, once the investor is 'signed up', to show the investor's fictitious return on investment.

   ASIC's use of s313 has been exclusively in response to cold-calling frauds. ASIC has used s313 to block websites linked to investment scams with the principal purposes of preventing access to those sites by Australian investors and disrupting the business models of the perpetrators as well as furthering ASIC's investigations into breaches of the law.

2. Our experience using s313 to block websites, along with subsequent media releases warning consumers about the fraud, indicates that it is a useful measure for disrupting investment frauds and warning Australian investors that the investment being offered is not legitimate.

   Importantly, the use of this section allows for very fast disruption, with notices to the telecommunications providers and subsequent blocking of the websites often taking place within hours of ASIC becoming aware of the scam. Given the speed at which the fraudsters move money out of accounts such that it becomes uncollectable, it is vital that ASIC can act quickly to protect Australian investors funds.

   While ASIC does not have empirical data regarding the use of fraudulent websites in cold calling scams, it does appear, from the level of complaints lodged with ASIC, that there has been a significant reduction in such scams since July 2013, a few months after ASIC last used this method to disrupt such activity.

   Submissions to the Inquiry have discussed the ease with which the blocking of websites can be circumvented. In this regard, it must be remembered that the operators of these fraudulent websites aim to reach as many potential victims as possible in as short a time as possible. To this end, it is less likely that they will use tools that make it difficult for their sites to be detected (as child pornography site operators may do).

   It must also be remembered that ASIC uses a range of methods in which to disrupt such frauds on Australian investors. ASIC will also take injunctive action and freeze bank accounts where possible, issue media releases warning consumers about such frauds and conduct covert investigations aimed at bringing the criminals to account. Together with the use of s.313 ASIC has been able to reduce the impact of such frauds.

3. ASIC has received legal advice, which is privileged, which confirms that ASIC is able to use s.313 in the manner and for the purpose which ASIC has used the section.

4. The purpose for which ASIC uses s.313 is to disrupt, as quickly as possible, fraudulent websites which are deceiving Australian investors out of their money. Such websites are hosted outside of Australia and often in jurisdictions where regulation is not as stringent as it is in Australia.

   One alternative action, suggested in a number of submissions to the Inquiry, to the use of s. 313 is for Court orders to be sought, pursuant to which the websites must be shut down. The disadvantages of such action as against the use of s. 313 are that injunctive orders or warrants of some form, no matter how urgent they are sought, take some time to obtain. Evidence must be prepared in appropriate form and filed; a Court hearing must take place; and the eventual orders must be served on a person or entity that can shut down the website. These persons are generally operating outside Australia, are difficult to locate and are not necessarily subject to Australian Court jurisdiction. This will delay the blocking of access to the website during which time more Australian investors will be at risk of losing their money. Further, such action comes at a cost to ASIC which

must pay for the Court application and often for legal Counsel to provide advice and appear on ASIC's behalf.

For example, in the Secured Private Wealth matter, ASIC commenced its investigation on 11 October 2012 upon receipt of investor complaints. While ASIC made a s313 request on 16 October to have the offending website blocked for 1 month, it was not until 18 October that ASIC obtained interim Supreme Court Orders. Those orders restrained three individuals and three companies from promoting investments and also froze $273,000 in three bank accounts. ASIC identified that $708,000 had already been withdrawn from those accounts prior to the orders being put in place (including prior to the commencement of the investigation). Overall, in excess of $15,000 was expended by ASIC on Counsel and court costs.

It must be noted that ASIC will, prior to making any request for access to a website be blocked, ensure that it is satisfied that the operators do not hold the requisite Australian Financial Services licence for the business being fraudulently advertised and undertake other checks of ASIC's own databases to ensure that there is likely to be the commission of a criminal offence. To date, ASIC has not been challenged by the operators of any fraudulent financial services website that has been the subject of a blocking request.

ASIC will, where money is identified in bank accounts in Australia as part of these frauds, seek urgent injunctions to freeze these accounts. As stated in the evidence given by ASIC to the Committee on 3 December, Australian Banks are cooperative in relation to these matters and will look to protect Australian investors' money that is at risk of such funds when approached by ASIC. In circumstances where ASIC does seek injunctions freezing accounts, it may also use s.313 to block access to the fraudulent websites as well.

5 In the past ASIC has not used block pages to alert users to the fact that the page the use is seeking to access has been blocked at the request of ASIC. As noted in our submission, ASIC supports taking steps to increase the transparency and accountability around the use of s.313, including the use of such notification pages.

6 The circumstances concerning the inadvertent blocking of websites in 2013 are:

On or about 26 March 2013, ASIC became aware that a serial fraud offender(in fact an offender who had recently been the subject of an ASIC civil injunctive action) had recommenced operating through two fraudulent websites and requested a number of telecommunications carriers block the IP addresses.

On or about 3 April 2013, ASIC became aware that the same serial offender had recommenced operating another fraudulent website and requested a number of telecommunications carriers block access to that IP address.

On the evening of 11 April, one of the carriers that had received ASIC's request advised us that connectivity to the website of Melbourne Free University had been affected as a result of the block requested on 3 April. In response, on the

morning of 12 April, ASIC requested the telecommunications carriers lift the block.

We were subsequently advised that the IP address hosted approximately 1090 websites, including that of the fraudulent financial services entity and that of the Melbourne Free University.

Once we became aware of the risk that our s313 blocking requests could result in the inadvertent blocking of websites we reviewed our procedures to identify how this was able to occur. Our internal review identified that: the ASIC teams requesting s313 blocks were not aware that a single IP address can host multiple websites; and to prevent inadvertent blocking of websites in any future s313 request, the responsible ASIC team should:

(a) liaise with ASIC's Evidence Services—Forensic team to ensure the information provided to the ISP facilitates the blocking of a specific website only; and

(b) work closely with the relevant telecommunications carriers to ensure that blocks are actioned effectively and responsibly, including that only the targeted website is blocked.

We also undertook a review of other s313 requests to ascertain whether other non-fraudulent websites had been blocked. This review alerted us to an IP address that hosted in excess of 250,000 websites. A further review indicated that in excess of 99.6% of these sites contained no substantive content. This blocking request was removed.

Apart from Melbourne Free University, ASIC has not been contacted by any other operator of the websites impacted.

ASIC has not made a s313 blocking request since April 2013.

7 No prosecutions have eventuated from the blocking of websites by ASIC.

However, ASIC understands that one person who has been charged by the Queensland Police in relation to a number of boiler room scams has been associated with 3 of the websites which ASIC requested be blocked. In this regard, ASIC has, and continues, to work closely with police authorities around Australia in relation to boiler room scams.

Yours sincerely

Greg Tanzer
Commissioner