ASIC
Australian Securities & Investments Commission

Inquiry into subsection 313(3) of the Telecommunications Act 1997: Submission by ASIC

August 2014

ASIC's submission

1 ASIC welcomes the opportunity to contribute to the inquiry into s313(3) of the *Telecommunications Act 1997* (Telecommunications Act).[1] Our submission provides information on ASIC's role and responsibilities, and ASIC's use of s313 to block access to websites linked to investment fraud. Our submission also addresses each of this inquiry's terms of reference.

2 The use of s313 for purposes other than blocking online content is outside the scope of our submission.

ASIC's role and responsibilities

3 ASIC regulates Australian companies, financial markets, financial services organisations, and professionals who deal and advise in investments, superannuation, insurance, deposit taking and credit.

4 The *Australian Securities and Investments Commission Act 2001* (ASIC Act) requires ASIC to:

(a) maintain, facilitate and improve the performance of the financial system and entities in it;

(b) promote confident and informed participation by investors and financial consumers in the financial system;

(c) administer the law effectively and with minimal procedural requirements;

(d) enforce and give effect to the law;

(e) receive, process and store, efficiently and quickly, information that is given to us; and

(f) make information about companies and other bodies available to the public as soon as practicable.

5 As the financial services regulator, we have responsibility for investor and consumer protection in financial services. We administer the Australian financial services (AFS) licensing regime and monitor financial services businesses to ensure that they operate efficiently, honestly and fairly. These businesses typically deal in superannuation, managed funds, deposit and payment products, shares and company securities, derivatives and insurance.

6 As the consumer credit regulator, we license and regulate people and businesses engaging in consumer credit activities (including banks, credit unions, finance companies, and mortgage and finance brokers). We ensure

[1] In this submission, 's313' means s313(3) of the Telecommunications Act.

that licensees meet the standards—including their responsibilities to consumers—that are set out in the *National Consumer Credit Protection Act 2009* (National Credit Act).

7 As the markets regulator, we assess how effectively financial markets are complying with their legal obligations to operate fair, orderly and transparent markets. We also advise the Minister about authorising new markets. On 1 August 2010, we assumed responsibility for the supervision of trading on Australia's domestic licensed equity, derivatives and futures markets.

8 As the corporate regulator, we ensure that companies, schemes and related entities meet their obligations under the *Corporations Act 2001* (Corporations Act). We register and regulate companies at every point from their incorporation through to their winding up, and ensure that company officers comply with their responsibilities.

9 ASIC also promotes financial literacy, to ensure investors can have greater confidence when buying financial services, and are able to make sensible and informed financial decisions.

ASIC's approach to disrupting investment fraud

10 As the financial services regulator we play a leading role in combatting investment fraud targeting Australian investors. Investment fraud often involves breaches of the Corporations Act—for example, offering a financial service without a licence (s911A).

11 In the period September 2009 to April 2013, ASIC conducted investigations into at least 17 cases of 'cold calling' investment fraud—colloquially known as 'boiler room' fraud—amounting to in excess of $8 million in losses to Australian investors.

12 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 generally 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.

13 These investment frauds are particularly difficult to disrupt as:

(a) detection of the perpetrators of these scams is very difficult due to the use of numerous false identities and addresses, prepaid credit cards obtained with false identity information, and employment of intermediaries who incorporate companies and open bank accounts from which investor funds are withdrawn in cash and paid to the scam organisers. These techniques effectively insulate the perpetrators from law enforcement identification; and

© Australian Securities and Investments Commission August 2014

(b) the websites used to support the fraud are typically hosted through overseas internet service providers (ISPs). In ASIC's experience, these ISPs do not always comply with ASIC requests to cease hosting the fraudulent website. If the ISP does comply, the perpetrators quickly become aware and change ISPs, with the website spending very little time offline.

14 Given the difficulty in identifying and apprehending the perpetrators of these frauds, ASIC instituted a number of strategies to disrupt their activities and warn Australian investors of the risks posed by these scams including:

(a) issuing consumer alerts or public warning motices through the media and posts such warnings on our MoneySmart website (these consumer alerts and media releases note, where relevant, that ASIC is or has taken steps to block access to the offending website or websites); and

(b) using s313 to block access from Australia to overseas hosted websites linked to these frauds.

ASIC's use of s313

15 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 on 10 separate occasions: see the appendix.

16 In general, when a website is blocked as a result of our s313 request we will issue a media release to warn consumers about the of the fraud. We have also used s313 requests to block websites following court orders that the perpetrators of the fraud 'deactivate' or 'cease the use of' the false website. Section 313 is a useful tool in these circumstances, as court orders are routinely frustrated by the fact that perpetrators are based overseas and have no intention of complying with the order.

17 Our experience using s313 to block websites indicates that it is a useful measure for disrupting investment frauds and warning Australian investors that the investment being offered are not legitimate. However, our use of s313 has also highlighted the risk that other websites may be inadvertently blocked in the process.

Example: Inadvertent blocking—Melbourne Free University

On or about 26 March 2013, ASIC became aware that a serial fraud offender 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.

© Australian Securities and Investments Commission August 2014

> 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. In response 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.

18 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.

19 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.

20 We have not made a s313 blocking request since April 2013. ASIC's current approach is to request voluntary suspension of any fraudulent websites and domain names through correspondence to the hosting ISP and domain name registry. ASIC will also consider issuing a consumer alert or public warning notice. ASIC will consider re-using s313 following appropriate consultation with other relevant agencies such as the Australian Federal Police (AFP) and with the telecommunications carriers.

Inquiry's terms of reference

21 This section addresses each of the Committee's terms of reference.

Which government agencies should be permitted to make requests under s313 to disrupt online services?

22 Agencies that have responsibility for enforcing the laws for which blocking is available should have the ability to make s9+313 requests. This approach facilitates timely action once fraudulent websites are detected. The ability of

© Australian Securities and Investments Commission August 2014

responsible agencies to respond quickly is an important consideration. For example, in relation to investment frauds, Australian investors will be exposed, and at risk of losing money, while the offending website remains accessible. Alternative approaches, such as requiring requests to go through a 'central agency', can have a negative impact on agencies' ability to block offending websites in a timely manner, without necessarily providing significant improvements in either transparency or accountability.

23 The Committee may wish to consider the whether the approach taken in the *Telecommunications Interception and Access Act 1979* (TIA Act) in relation to specifying agencies that can apply for stored communications warrants is a useful model. Under the TIA Act an 'enforcement agency'[2] may apply for a warrant to access stored communications. The definition of 'enforcement agency' includes any body whose functions include administering a law imposing a pecuniary penalty or a law relating to the protection of the public revenue. ASIC is specifically identified as an enforcement agency in the TIA Act.

What level of authority should agencies have for making s313(3) requests?

24 Agencies should continue to be responsible for authorising their own notices under s313. However, the level of authorisation required within each agency is an important accountability measure and must be limited to an appropriate number of senior staff. Again, the level of authority required needs to be balanced against the ability for the agency to take timely action once an illegal website is detected.

25 The Committee may wish to consider the whether the approach taken in the TIA Act is a useful model. The TIA Act provides that the chief officer of an enforcement agency can make an application for a stored communications warrant and nominate officers or positions involved in the management of the agency to make such applications (the ASIC Chairman has nominated a member of the Commission, the Regional Commissioner for each state and territory, and ASIC's Senior Executive Leaders).[3]

What characteristics of illegal or potentially illegal online services which should be subject to s313 requests?

26 The blocking of content under s313 should only be used in cases of serious criminal activity or the risk of serious harm to Australians with any threshold being clearly articulated (e.g. criminal activities subject to an offence with a statutory maximum penalty of at least two years imprisonment).

[2] TIA Act, s5.
[3] TIA Act, s110(3).

27 Importantly, the threshold set out in paragraph 26 would include blocking websites that are linked to investment fraud (i.e. where s911A, s1041G, s1041F of the Corporations Act are breached or suspected of being breached). Investment fraud can have a significant impact on Australians and the risk is expected to increase over the next 20 years, given the ever-growing pool superannuation investments, as the following extract from an Australian Crime Commission fact sheet[4] suggests:

> **Extent**
>
> Based on initial indications, more than 2600 Australians have lost in excess of **$113 million** to investment frauds (between January 2007 and April 2012), but it is believed there is a high level of under-reporting and the extent is far greater.
>
> Organised criminal groups are attracted to the high levels of superannuation and retirement savings in Australia. The Australian economy is known to have been less affected by the global financial crisis than other nations, making those approaching retirement an attractive target.
>
> In the next 20 years, a large number of Australians are expected to retire from active work and will have superannuation investments to manage. Raising awareness of serious and organised investment frauds is important in preventing people falling victim.
>
> **Impact**
>
> Victims have lost significant amounts of money and in some cases, all of their retirement funds. Reported individual loss ranges from $35 000 to more than $4 million. This loss can have a profound negative impact on an individual and family's wellbeing. The financial and social impact also has wider implications for the community and government services, and the Australian economy suffers as funds that might otherwise be invested here are diverted overseas.
>
> Victims of serious and organised investment frauds may be embarrassed and unwilling to report their loss, even though they have been targeted by organised crime operations, using sophisticated techniques specifically designed to entrap them. An unwillingness to disclose a fraud can cause further problems in the victim's personal life. Under-reporting of fraud also reduces the evidence base available to law enforcement and government authorities and can hamper efforts to prevent further fraudulent activity.

28 Given the difficulties in disrupting investment frauds, particularly those based overseas, it is critical that ASIC has at its disposal an effective and flexible enforcement toolkit, including the ability to block illegal websites.

[4] Australian Crime Commission, *Serious and organised investment frauds*, www.crimecommission.gov.au/publications/intelligence-products/crime-profile-fact-sheets/serious-and-organised-investment-frauds.

What are the most appropriate agency transparency and accountability measures?

29 ASIC supports taking steps to improve the transparency and accountability around the use of s313.

30 Some measures that the Committee may wish to consider were set out in the Department of Communications draft consultation paper[5] that was prepared, in consultation with a range of government agencies including ASIC, earlier this year.

31 The draft consultation paper proposed that agencies that intend to use s313 adhere to the following set of whole-of-government principles to govern this use:

(a) Blocking of online content by Australian Government agencies should be transparent and based on the international human right to freedom of expression. Where blocking occurs, it should be consistent with international law, and only be used where there is a strong and demonstrable public benefit.

(b) Content blocking must be restricted to material that represents either serious criminal activity or a threat to national security. Use of an information page (but without blocking access to content) should only be used where there is a risk of serious harm to Australians.

(c) Agencies intending to block content or provide information pages under s313 should develop clear blocking policies that outline the types of content they intend to target and the processes and procedures that govern their use of s313. These policies should be consistent with the agreed whole-of-government approach to blocking and be available for appropriate scrutiny. As part of this process, approval of the blocking policy should also be sought from the agency head (or Minister if appropriate).

(d) Before an agency uses s313 to implement a policy of blocking content and/or using information pages, it should consult with relevant Australian Government agencies and ISPs to ensure that blocks and information pages are actioned effectively and responsibly, and that an appropriate approach is taken. In most cases, blocking requests should specify an end date. Where this is not specified, measures (such as annual review) should be in place to ensure that the block remains valid.

(e) The agency blocking policy should specify which senior officers within the agency can request blocks and issue information pages, and include procedures for seeking legal advice before making each request.

[5] Department of Communications, *Improved transparency and accountability when blocking online content via section 313 of the Telecommunications Act 1997*, draft consultation paper, December 2013, unpublished.

(f) Agency blocking policies should outline the internal review processes the agency has in place to facilitate a quick resolution of appeals against a particular block or information page. This should include processes for the quick reinstatement of access to online content where a block is found to be inappropriately targeted.

(g) Where operational circumstances and/or security sensitivities allow, agencies should publicly announce through an appropriate medium each instance of requesting a block or issuing an information page. This should include, where appropriate, an explanation of why the block or information page was put in place.

(h) Blocking and/or information page requests should be accompanied by a notification page that the user would see when trying to access the relevant website. This page should, at a minimum, state that the action has been taken by the Australian Government and, where possible, include a reason. An agency contact point should be provided for further information.

(i) The Australian Communications and Media Authority (ACMA) should maintain a list of agencies which use section 313 to block or provide information pages with regards to online content. ACMA should also report publicly on the extent of blocking activities under s313 by agencies.

© Australian Securities and Investments Commission August 2014

Appendix: Section 313 blocks requested by ASIC

Date of s313 request	Period requested	Website(s)	Court orders and ASIC media releases
26 June 2012	1 month	Deutsche Capital	None
16 October 2012	1 month	Secured Collateral	Court Orders 18/10/2012 12-265MR *ASIC obtains orders freezing bank accounts of Brisbane 'cold callers'* (1 November 2012)
23 November 2012	1 month	Swiss Private Capital	12-293MR *ASIC warns consumers against purported investment firm* (28 November 2012)
19 December 2012	1 month	Prestige Private Wealth	12-329MR *ASIC warns consumers about Prestige Private Wealth* (20 December 2012)
9 January 2013	1 month	China Environmental Group	None
15 February 2013	1 month	Swiss Private Capital and Swiss Union	12-293MR
14 March 2013 (Repeat of 9 January 2013 request)	Until further notice per court orders	China Environmental Group	Court Orders 13/3/2013 14/3/2013 14/5/2013 13-053MR *ASIC acts to stop offshore scam netting Australian investors* (19 March 2013)
18 March 2013 (On 26 March 2013 the same request was sent to another carrier)	1 month	Global Capital Wealth and Global Capital Australia	13-061MR *ASIC warns consumers about Global Capital Wealth* (22 March 2013)
26 March 2013 (Repeat of 15 February 2013 request)	3 months	Swiss Private Capital and Swiss Union	12-293MR
3 April 2013	2 months (removed on 11 April)	Global Capital Wealth and Global Capital Australia	13-061MR