A S I C
Australian Securities & Investments Commission

Jillian Segal, Deputy Chair, Australian Securities and Investments Commission, comments on Debra A Valentine's paper, "Regulating in a high-tech marketplace –the import for remedies"

Australian Law Reform Commission Conference, "Penalties: Policy, Principles & Practice in Government Regulation", 7-9 June 2001

Introduction

- The characteristics of the financial sector in the 21st century (i.e. the "hallmarks of the high-tech marketplace" of which Debra spoke) such as globalisation and rapid change result in the need for flexible, timely and effective remedies.
- The relative speed and ease with which things can be communicated on the Internet means that it is more important than ever that regulators move quickly against scams, and that they be innovative and resourceful in their approach to regulation.
- Therefore, like the Federal Trade Commission (FTC), the Australian Securities and Investments Commission (ASIC) has also sought to use the powers and remedies available to it in creative ways – e.g. increasing its use of administrative remedies (such as enforceable undertakings (EUs), licensing powers and banning orders) in place of civil and criminal action where the same outcome can be achieved more quickly, as well as welcoming some proposed additions to its regulatory toolkit.
- This morning, I would like to comment briefly on the following:
  1) Civil Penalties;
  2) Administrative remedies including EUs, licensing, and banning; and
  3) Other approaches to deal with e-offences and issues in the "new economy".

Civil Penalties

Background

- Civil penalties were first introduced into the *Corporations Law* (CL) by the *Corporate Law Reform Act 1992 (Cth)* (effective 1 February 1993). Initially, civil penalties were limited to breaches of directors' duties, liability for insolvent trading, failure to ensure compliance with financial reporting, related party transactions, share capital transactions and breaches of responsible entities' duties.
- *The Company Law Review Act 1998 (Cth)* – extended the operation of the civil penalty provisions (CPPs) to liability with respect to certain share capital provisions and managed investment schemes.
- Certain changes were also made by the *Corporate Law Economic Reform Program Act 1999 (Cth)* (CLERP) (effective 13 March 2000) – e.g. previously, the commencement of proceedings for a civil penalty order acted as a bar to subsequent prosecution for the corresponding criminal offence (old section 1317FB CL). Under these circumstances, it was obviously a disincentive for ASIC to commence civil penalty proceedings. As a result of CLERP, section 1317P CL (which replaced section 1317FB CL) now states that criminal proceedings can be commenced against a person for the same conduct, regardless of any civil penalty orders that have been made (although, evidence given in the course of proceedings for a pecuniary penalty order is not admissible in criminal prosecutions – section 1317Q CL).

The expansion of the civil penalty regime

- ASIC welcomes the expansion of the civil penalty regime under the *Financial Services Reform Bill 2001 (Cth)* (FSR Bill) to market misconduct (proposed Part 7.10) and continuous disclosure matters (proposed Chapter 6CA). This means that contraventions of the market misconduct and continuous disclosure provisions will be subject to both civil penalties and criminal consequences.
- The ability to institute a quick regulatory response to contraventions of the market misconduct and continuous disclosure provisions is particularly important because these types of contraventions have an immediate impact on the market and as such need to be rectified immediately.

- Debra spoke about the use of civil penalties for non-compliance with disclosure or notification obligations. Under the FSR Bill, it is proposed that the civil penalty remedy be extended to the continuous disclosure regime. ASIC has long supported the extension of the civil penalty remedy to market offences including continuous disclosure. The very basis underpinning the continuous disclosure regime is the provision of price sensitive information to the market in a timely fashion. If a company fails to disclose such information to the market in breach of the continuous disclosure provisions, the availability of civil penalties is significant for two reasons:
  (i) the mental elements that need to be proved in a criminal proceeding is a high bar for the prosecution; and
  (ii) the outcome achieved by criminal prosecution is too late to rectify the harm caused to the market and its participants. Of course, criminal action may be effective in deterring future misconduct. However, the damage to the market may be better rectified by other means (e.g. civil penalties). In any event, it is important that civil penalties are available to the regulator (in addition to criminal remedies) as an option.

Examples of breaches of the continuous disclosure provisions

- Currently, civil penalties are not available in relation to breaches of the continuous disclosure regime (although as already mentioned, the civil penalty regime is extended to continuous disclosure breaches under the FSR Bill). Therefore, in the absence of civil penalties, ASIC has opted to use enforceable undertakings in response to continuous disclosure breaches. Some examples are as follows:

Plexus International Limited (Plexus)

- ASIC accepted an EU from Plexus, a West Australian-based technology company, on 5 April 2001.
- ASIC received the undertaking after raising concerns about Plexus' compliance with its continuous disclosure obligations under the Australian Stock Exchange (ASX) Listing Rules and the CL.
- The enforceable undertaking requires Plexus to review its internal procedures for ensuring compliance with its continuous disclosure obligations, and to have those

procedures independently audited by a senior member of the corporate finance industry. It also requires Plexus to review, formalise and annually audit its corporate governance practices.

Pahth Telecommunications Limited (Pahth)

- ASIC accepted an EU from Pahth, also a West Australian-based technology company, on 2 February 2001.
- ASIC received the undertaking after raising concerns about Pahth's compliance with its continuous disclosure obligations under the ASX Listing Rules and the CL.
- The enforceable undertaking requires Pahth to review its internal procedures for ensuring compliance with its continuous disclosure obligations, and to have those procedures independently audited by a senior member of the stockbroking profession. It also provides for Pahth to review, formalise and annually audit its corporate governance practices.

Administrative remedies

- Debra has commented on the usefulness of some of these remedies to the FTC in particular contexts. Whilst I agree that administrative remedies can be no substitute for urgent civil action at the initial stages of an investigation, ASIC has still found administrative remedies to be a speedy alternative to, or supplement for, final civil proceedings.
- When ASIC commences action in relation to a matter, its first priority is always to protect the interests of consumers and investors quickly and adequately. It is therefore important to choose a remedy that can achieve an effective outcome quickly, and that is appropriate to the particular circumstance. Consequently, it is important for the regulatory agency to have the flexibility to choose the most appropriate remedy.

Enforceable undertakings

Background

- ASIC's power to accept EUs is relatively new. It came into force on 1 July 1998 when the Australian Securities Commission (ASC) became the Australian Securities and Investments Commission (ASIC) as a result of the enactment of the

Financial Sector Reform (Amendments and Transitional Provisions) Act 1998 (Cth).

- ASIC's power to accept EUs is contained in sections 93AA (generally) and 93A (in relation to registered managed investment schemes) of the *Australian Securities and Investments Commission Act 1989 (Cth)* (ASIC Act – which is also referred to as the ASC Law in Practice Note 69 discussed below).
- EUs are similar to the ACCC's power in section 87B of the *Trade Practices Act 1974 (Cth).*

ASIC's Practice Note 69 – Enforceable Undertakings

- In this Practice Note, ASIC states its views on the policy, interpretation and operation of sections 93A and 93AA of the ASIC Act. Part A explains when ASIC will accept EUs under sections 93A and 93AA of the ASIC Act. Part B provides examples of acceptable and unacceptable terms in EUs. Part C describes what happens if an EU is not complied with and Part D sets out when ASIC will consent to a request to vary or withdraw an EU.

Part A: When ASIC will accept enforceable undertakings

- Sections 93A and 93AA of the ASC Law commenced operation on 1 July 1998. ASIC may accept a written EU either:
  (a) in connection with a matter in relation to which it has a function or power under the ASC Law (section 93AA); or
  (b) given by a responsible entity of a registered scheme in connection with a matter concerning the registered scheme, and in relation to which ASIC has a function or power under a national scheme law (section 93A).

- In general terms, ASIC has functions and powers conferred on it by the:
  (a) CL;
  (b) ASC Law;
  (c) *Insurance Act 1973 (Cth)*;
  (d) *Insurance (Agents and Brokers) Act 1984 (Cth)*;
  (e) *Insurance Contracts Act 1984 (Cth)*;
  (f) *Superannuation (Resolution of Complaints) Act 1993 (Cth)*;

(g) *Life Insurance Act 1995 (Cth)*;

(h) *Retirement Savings Accounts Act 1997 (Cth)*; and

(i) *Superannuation Industry (Supervision) Act 1993 (Cth).*

- An EU can be initiated by a company, an individual or a responsible entity (Promisor) or as a result of a discussion between that party and ASIC. However, ASIC does not have the power under sections 93A and 93AA to require a person to enter into an EU. Similarly, a person cannot compel ASIC to accept an EU.

Nature of an enforceable undertaking

- ASIC may accept an EU instead of taking proceedings for a civil order from a Court (e.g. an award of damages or compensation, or an injunction) or taking administrative action (e.g. imposing conditions on a licence) or referring a matter to other bodies (e.g. to the Companies Auditors and Liquidators Disciplinary Board (CALDB) or the Corporations and Securities Panel (CSP)). However, it is more versatile than any of those remedies, and may be used to achieve outcomes which might not be available by those means, and which are more focused (e.g. adoption of a compliance regime, restriction of a person's securities business or practice as an auditor).
- An EU is different from an undertaking to the Court. The main differences between an undertaking to ASIC and an undertaking to the Court are that:
  (a) an undertaking to the Court may only be given when a Court action has been commenced. ASIC does not have to commence Court action before it can accept an undertaking under the ASC Law (sections 93A or 93AA); and
  (b) a breach of an undertaking to the Court may itself be the subject of contempt proceedings.

Accepting enforceable undertakings

- ASIC will generally only consider accepting an EU when:
  (a) it has considered starting civil or administrative enforcement action in respect of a contravention or an alleged contravention of the relevant legislation by a party; and

(b) it considers the undertaking to be an appropriate regulatory outcome having regard to the significance of the issues concerned to the market and the community.

- Other factors which ASIC will consider when deciding whether accepting an EU is an appropriate regulatory outcome, include:
  (a) whether a person is likely to comply with it (any history of complaints involving the Promisor may be relevant);
  (b) whether a person is prepared to acknowledge that ASIC has reason to be concerned about the alleged breach;
  (c) the nature of the alleged breach and the regulatory impact of the undertaking compared to that of the other forms of enforcement remedy; and
  (d) the prospects for an expeditious resolution of the matter.

Civil or administrative proceedings

- ASIC will not always accept an EU instead of commencing or settling existing civil or administrative proceedings. In appropriate cases, ASIC may accept a Promisor's EU if that would be a complete settlement of existing or potential civil or administrative enforcement action.

Pecuniary civil penalty

- Often ASIC will not accept an EU where a pecuniary civil penalty may be payable or reference to a specialist tribunal (e.g. CALDB/CSP) may be more appropriate.

Examples

- The following examples are described in general terms to illustrate the circumstances in which ASIC may accept an EU. Every EU is tailored to the particular circumstances of the matter and will contain specific undertakings clearly setting out the Promisor's obligations. ASIC may accept an undertaking from the Promisor that it will:
  (a) pay damages to identified third parties, along with a description of the process for bringing this about;
  (b) refrain from taking part in the management of a certain corporation for a set period of time;

(c) remove a website at which securities advice is given by an entity contrary to the CL and to refrain from replacing it with a website falling within defined parameters;

(d) cease promoting an illegal fundraising scheme and/or to bring the scheme into compliance with relevant provisions of the CL within a defined period of time;

(e) amongst other things, inform the market to correct some previous false or misleading disclosure or any continuing misapprehension for which it is responsible;

(f) set up and implement an internal compliance plan and to report periodically to the market;

(g) refrain from acting as a broker without a licence in contravention of the *Insurance (Agents and Brokers) Act 1984 (Cth)*;

(h) remedy the deficiencies in the company's structure and administration system by taking certain specified action;

(i) compensate the beneficiaries of a superannuation entity for any loss suffered as a result of its misleading conduct whilst acting as trustee;

(j) remedy the unacceptable circumstances which have, or may have occurred in relation to a takeover by carrying out certain necessary action (provided that the matter has not been referred to the CSP; and

(k) perform a community service obligation (e.g. to increase consumers' knowledge of particular financial services).

Part B: Terms of enforceable undertakings

Acceptable and standard terms

- ASIC will only accept an EU when the Promisor makes a positive commitment to:
  (a) stop the particular conduct or alleged breach that concerns ASIC; and
  (b) not recommence that conduct.
- An EU must also set out how the Promisor will:
  (a) address the conduct ASIC is concerned about;
  (b) prevent that conduct occurring again; and/or
  (c) rectify the consequences of the conduct.

- An EU must set out what the Promisor is going to do to ensure that the conduct does not occur again. This may include:
  (a) details of the monitoring and reporting mechanisms it will adopt (e.g. developing internal control/compliance programs);
  (b) the name of the contact officer who is responsible for monitoring and complying with the undertaking; and
  (c) the name of an ASIC officer to whom the contact officer must report.
- In resolving any matter ASIC wants to find ways to undo the harm caused by the alleged breach. This may involve the Promisor compensating, reimbursing or giving other appropriate forms of redress to parties adversely affected by its conduct.
- In cases of misleading conduct, ASIC will require the Promisor to unequivocally correct the misapprehension for which it is responsible.

Publicity and public access to undertakings

- ASIC will generally not accept enforceable undertakings in confidence unless ASIC believes:
  (a) it is commercial in confidence; or
  (b) it would be against the public interest to do so; or
  (c) it contains personal details of an individual.
- Anyone can access copies of EUs from ASIC's ASCOT database (via its online agents and Business Centres). When an EU is given by a listed company, Listing Rule 3.1 of the ASX Listing Rules and section 1001A of the CL may require the company to release a copy of the undertaking to the ASX.

Unacceptable terms

- Generally, ASIC will not accept an EU if it contains a clause denying liability or it omits any of the standard clauses listed in paragraph 33 of Practice Note 69 (unless otherwise specifically excluded by ASIC).
- ASIC will not accept an EU if it contains any clause that sets up defences for possible non-compliance with an EU.

Part C: What happens if an enforceable undertaking is not complied with

- If ASIC believes or has been advised that a Promisor has not complied with a term of an EU, ASIC may apply to the Court for appropriate orders.
- A breach of an undertaking given to ASIC under sections 93A or 93AA of the ASC Law cannot itself be the subject of contempt proceedings. However, a breach of a Court order granted because of a breach of the EU may constitute a contempt of Court.

Examples of EUs

- Since the inception of ASIC's power to use EUs on 1 July 1998, 132 EUs have been accepted by ASIC in a wide range of circumstances including; listed company's failure to comply with its continuous disclosure obligations; failure to lodge annual returns and keep proper accounting records; failure to perform properly the duties of a securities dealer or investment advisor efficiently, honestly and fairly; deficiencies in offer information statements; and illegal fundraisings by managed investment schemes (e.g. no prospectus or trust deed, promoters not licensed).
- EUs have also been particularly suitable for dealing with a range of Internet related behaviour including; provision of unlicensed investment advice (including on the Internet); making of misleading and deceptive representations (e.g. billboard advertisements in relation to product liability, representations about securities on website noticeboards); illegal fundraisings (including on the Internet); and operation of Internet share investment games by managed investment schemes.
- Furthermore, the EUs have ranged from dealing with large corporations to individuals. Some examples include:

(1) Westpac Banking Corporation (Westpac)

- On 16 December 1999, ASIC accepted an EU from Westpac.
- ASIC considered that in its Advisory Services Guide (AGS), Westpac did not make the level of disclosure to its retail investment customers required by the CL.
- Westpac undertook to amend a number of consumer disclosure documents (including the AGS) and have them reviewed by a consumer consultant.

(2) Crown Limited (Crown)

- On 11 September 1998, ASIC accepted an EU from Crown after ASIC alleged that Crown had breached the continuous disclosure provisions of the CL and the ASX Listing Rules.
- The EU provided that Crown would implement a detailed internal compliance program that would be overseen by a Compliance Committee including non-executive directors of the company.

(3) Dymatech Pty Ltd (Dymatech)

- On 8 February 2001, ASIC accepted an EU from Dymatech and its director, Geoffrey Newton Day, as a result of concerns that Dymatech was not appropriately licensed to provide investment advice.
- Dymatech acted as an Internet based investment advisor, publishing information and recommendations concerning securities and futures commodities on a website that was accessible to its clients. Dymatech attracted 23 clients who paid $73,000 in subscription fees to access the website.
- The EU ensured that Dymatech would not recommence publishing this type of information until it was appropriately licensed.

(4) Ernest Alfred Brown

- On 2 March 2000, ASIC accepted an EU from Ernest Alfred Brown, a former director of Kenna and Brown Pty Ltd.
- In the EU, Mr Brown undertook not to be a director, secretary or be involved in the management of a corporation until 2006. Mr Brown also undertook that he would satisfactorily complete a suitable corporate management training course approved by ASIC, before returning to the management of a corporation.

Licensing powers

- ASIC's licensing powers are a useful administrative remedy in its regulatory toolkit. Division 1 of Part 7.3 and Part 8.3 of the CL contains ASIC's powers to grant a dealers licence or an investment advisers licence, and its powers to grant a futures brokers and futures advisers licences respectively.

- Division 5 of Part 7.3 and Part 8.3 of the CL, contains ASIC's powers to exclude persons from the securities industry and from the futures industry respectively. Proposed Subdivision C of Division 4 of Part 7.6 of the FSR Bill provides ASIC with similar powers.
- Licensing in the "new" economy will be an important issue under the FSR Bill – particularly in relation to the licensing of those providing investment advice over the Internet and those operating Internet Discussion Sites (IDS's).
- For example, ASIC has created "safe harbours" within the licensing context in relation to IDS's. ASIC's Interim Policy Statement 162 "Internet Discussion Sites" (IPS 162) specifies standards of behaviour, which, if complied with, effectively creates a "safe harbour" from ASIC's licensing requirements. That is, the statement provides guidelines for the operation of IDS's without a licence. For instance, where IDS's are conducted by non-professionals and there are appropriate disclosures about the potential risks for consumers in relying on opinions posted on the site, IPS 162 gives relief from the present legislative licensing requirements of the CL. Otherwise, operators of chatsites and bulletin boards will need to be licensed by ASIC.
- ASIC's Policy Proposal Paper – *Licensing: The scope of the licensing regime: Financial product advice and dealing* provides guidance, in the form of general principles and illustrative examples, to assist people in determining whether they are providing advice or are dealing (e.g. telephone call centres, bank tellers and Internet portals) and related questions such as when they need to be licensed, what kind of licence they need, authorization issues, competency and training requirements, and conduct and disclosure obligations.

Banning orders

- Similarly, ASIC's banning powers have also been a useful administrative remedy in its regulatory toolkit.
- Banning orders are orders that effectively prohibit a person from doing an act as a representative of a dealer, or of an investment adviser, either permanently or for a specified period. Section 828 of the CL provides that subject to section 837 (in relation to the opportunity for a hearing), where ASIC revokes or suspends a

licence held by the person, it may also make a banning order against the person. ASIC may also make a banning order against an unlicensed person under section 829 of the CL (subject to a hearing). Division 8 of Part 7.6 of the FSR Bill proposes similar banning powers.

- ASIC's *Hearings Practice Manual* sets out the principles and procedures that ASIC adopts in conducting administrative hearings held for the purpose of giving a person their statutory right to be heard.
- ASIC delegates conducting administrative hearings are independent of the matter being heard and are guided by seven essential principles which include; the opportunity to be heard, the entitlement to a notice; the right to an impartial decision maker; findings of fact to be made on a sound basis; no onus of proof; court practice does not apply; and the application of policy and precedents.
- In the current financial year to date, ASIC has made 19 banning orders. Recent examples include: *Warren John Aitken (28 March 2001)* who was permanently banned from acting as a representative of a securities dealer or an investment adviser after ASIC found that Mr Aitken did not perform the duties of an investment adviser efficiently, honestly or fairly; and *Graeme John Perry (9 April 2001)* who was permanently banned from acting as a representative of a securities dealer or an investment adviser after ASIC found that Mr Perry had breached the CL by failing to make reasonable or adequate inquiries on behalf of investors, about the financial position of borrowers and guarantors and their ability to service investor loans.

ASIC's proactive, cooperative and consultative approach

- Debra has spoken about the need for coordination and communication among courts, civil and criminal enforcers, private attorneys, and victims. I agree that there must be careful coordination between the relevant groups (including regulators, industry and consumers) in order to ensure fair compensation to victims and prevent against over-deterrence.
- ASIC's approach to the Internet and e-commerce is driven by a desire to maintain a consistency of regulation within these new channels, and to look to the future as a real-time Cyber regulator. As such, ASIC has been innovative/proactive in response to developments in the "new economy".

Chairing working groups

- ASIC has demonstrated its proactive, co-operative and consultative approach in chairing various working groups. An example of this is ASIC's chairing of the group convened to review the *Electronic Funds Transfer Code of Conduct* (EFT Code) (launched on 5 April 2001). ASIC gathered representatives of industry and consumer groups together and, through effective chairing, has managed to have such a group agree a voluntary code governing behaviour that is presently outside the legislative regime. The EFT Code now extends to telephone banking, Internet banking and stored value products. Another example is ASIC's approach to developing the *"Guide to Good Transaction Fee Disclosure for Banks, Building Societies and Credit Unions"* (launched on 4 April 2001). The draft guide was developed by ASIC in conjunction with a working group of industry, consumer and government representatives.

Cybercrime proposals – amendment of the Crimes Act 1914 (Cth)

- ASIC has also participated in the Federal Government's Cybercrime initiative that proposes to amend the *Crimes Act 1914 (Cth)* (Crimes Act) by incorporating new offences, and enhancing criminal investigation powers to remedy the deficiencies in existing laws and enable law enforcement agencies to effectively combat computer crime.
- The proposed offences and enforcement powers are designed to protect the security, integrity and reliability of computer systems and will provide a stronger deterrent to those who engage in activities such as "hacking" and denial of service attacks.
- The proposed amendments to "criminal investigation powers" will be of great utility to ASIC as it will assist the process of collecting evidence to support the prosecution of new offences.

Offences

- It is proposed to amend the *Criminal Code* to create new computer offences to replace the existing offences in Part VIA of the Crimes Act. The new offences will subsume the existing offences, but provide more comprehensive coverage. The

proposed computer offences are based on the offences in the *Model Criminal Code* (agreed to by all State and Territory governments).

- The offences are generally directed at protecting computers and electronic data from unauthorised access, impairment and corruption, and carry maximum penalties of between two and ten years imprisonment. The offences have been framed so as to ensure consistency with the *Electronic Transactions Act 1999 (Cth)* (ETA Act) and, where appropriate, the terminology used in the proposed offences has been drawn from the ETA Act.
- The new offences cover unauthorised computer activities such as accessing commercial or confidential information commonly known as "hacking", denial of service, spreading computer viruses, unauthorised access with the intent to commit an offence and trading in technology designed to hack or damage another person's computer. It will also be an offence to commit a serious crime such as stalking or fraud by computer. The maximum penalty for these types of offences will be ten years imprisonment.

Law enforcement powers

- It is proposed to amend the Crimes Act to introduce new law enforcement powers and enhance existing powers in order to facilitate the detection and investigation of technology assisted crime. The proposed powers are modelled on the powers proposed in the Council of Europe draft Cyber-Crime Convention.
- Law enforcement powers will also be updated to include powers to access information stored on a hard drive in multiple locations, specialist off-site examination or copying of potential computer hardware and software for evidence, and the power to compel the owner of a computer to provide assistance in locating evidence on the computer.

Conclusion

- ASIC's priority is to protect the interests of consumers and investors as quickly and as effectively as possible. In order to achieve this objective, particularly in the "new economy", the regulator needs to have the flexibility to choose the most appropriate, timely and effective remedy.

- ASIC has increased its use of administrative remedies in its regulatory toolbox (e.g. EUs, licensing and banning powers) as they are often a speedy alternative to civil and criminal proceedings and achieve the desired regulatory outcome. This is particularly important in today's rapid paced economy.
- As a real-time Cyber regulator, ASIC's approach to issues arising in the "new economy" has been innovative/proactive. This is demonstrated by our involvement in chairing various working groups (e.g. revision of the EFT Code) and its participation in the Federal Government's Cybercrime initiative, which proposes to incorporate new offences and enhance criminal investigation powers in the Crimes Act.
- ASIC welcomes the expansion of the civil penalty regime under the FSR Bill to market misconduct and continuous disclosure matters and the aforementioned proposals to amend the Crimes Act. The availability of civil penalties and the expansion of investigation powers will be of great use to ASIC in counteracting cybercrime more effectively and efficiently in the new age.