

30 June 2004

IT and Telecommunications Policy Group  
Resources and Network Branch  
Ministry of Economic Development  
PO Box 1473  
Wellington

### **Legislating Against Spam Discussion Document**

These submissions are made on behalf of the members of the New Zealand Bankers' Association ("NZBA") namely:

ANZ National Bank Limited  
ASB Bank Limited  
Bank of New Zealand  
Citibank NA  
The Hongkong and Shanghai Banking Corporation Limited  
Kiwibank Limited  
TSB Bank Limited  
Westpac Banking Corporation (New Zealand division)

### **Introduction**

Thank you for the opportunity to make these submissions. The NZBA considers that Spam is a considerable problem, and that regulation of this activity would be welcomed. While the adoption of the Australian anti – Spam legislation in this jurisdiction has some attraction; the NZBA would suggest that the Ministry of Economic Development ("MED") carefully consider issues that have arisen in Australia for businesses because of clearly unintended consequences of the application of that legislation. Some of these issues are discussed below in the general comments section of these submissions. The NZBA would welcome further consultation and would be available to further discuss the issues to aid the MED in avoiding these problems with the New Zealand legislation.

### **Q1. Do you consider Spam to be an important issue? Has it significantly affected you in any way?**

The NZBA considers Spam to be a considerable issue – the figures quoted in the paper bear this out. NZBA members have been impacted by Spam in many ways, including from a business perspective (clogging servers etc), and from a fraud perspective, (keystroke logger programmes entering PC's through a spammed trojan). Another key issue is that the level of trust can deteriorate between the Bank and the customer; this is because the customer becomes unable to ascertain what is a legitimate bank email and what is fraudulent. This also reduces customers trust in online transactions generally as they choose to substitute towards more perceived "safer" channels for conducting transactions.

**Q2. Do you think legislation has a role to play alongside other complementary measures?**

The NZBA would support legislation designed to prevent Spam as part of a multidimensional approach so long as the legislation was designed to achieve the policy goals outlined at paragraph 20 of the discussion document, and there were adequate resources provided for the purposes of enforcement. The NZBA believes that the intent of the legislation, its scope and all definitions must be clearly defined before any legislation is drafted. It is imperative that an accurate and concise definition of Spam be debated and agreed together with all interested parties including organisations, corporate and business representatives.

In addition, the NZBA is concerned that the Ministry of Economic Development has indicated it is likely to base New Zealand's anti-Spam legislation on the recently enacted Australian Spam legislation.

Since its enactment, it has become evident that the scope of the Australian Act has gone well beyond capturing what is commonly known as 'spam' by including the broad definition of 'commercial electronic message' (one which offers to supply goods or services, advertise or promote a supplier of goods or services, offers to supply land or an interest in land, offers to provide or to advertise or promote a business opportunity or investment opportunity, assist or enable a person, by deception to dishonestly obtain a financial advantage from another person).

As a result, the Australian Act defines the problem of Spam as one thing and attempts to resolve a completely unrelated issue (i.e. the sending of legitimate marketing messages by legitimate business). The result, unfortunately, has been the steady decline in e-business and its development due to the increased compliance costs and required controls. Understandably, the legislation has been labelled a 'disproportionate solution to the Spam problem'.

The NZBA would encourage the Ministry of Economic Development to not only review the Australian legislation but to carefully assess the unintended impact of the Act on organisations and businesses. In particular, the Ministry should review the broad definition of 'commercial electronic message' and its effect on legitimate communications by business and individuals before adopting any of the Australian provisions.

**Q3. Do you consider existing privacy protections in this area sufficient?**

**Q4. Do you agree that stand-alone anti-Spam legislation is preferable to reliance on the Harassment Act?**

A3, and A4 The NZBA considers that specific anti Spam legislation would be preferable to a reliance on protections in the Privacy Act, or in the Harassment Act. While current domestic legislation might provide some protections, and penalties against spamming, these do not appear to be sufficient remedies in their own right and it is preferable, in light of the international nature of spamming that NZ legislation fits into the international regulatory environment to aid in restricting the practice.

**Q5. What message mediums should be caught by the legislation (e.g. email, short message services using mobile phones, Internet instant messaging, faxes, telephones (telemarketing), physical mail delivery)?**

The NZBA considers that the legislation should be directed at electronic mediums, because electronic bulk messaging is essentially costless to the marketer in sending their material numerous times to a limitless audience, and its receipt is difficult to prevent. Marketers conducting physical mail delivery and telemarketing should be exempted from the ambit of any SPAM legislation. These types of marketing incur costs – this restricts the use of these mediums to targeted marketing. Recipients of this type of marketing can utilize mechanisms

to prevent receipt, or to limit its receipt. For example the NZBA believes it would be inappropriate for any legislation to capture faxes as the Australian Spam Act 2003 does.

**Q6. Do the messages caught by the legislation have to be sent/conveyed to many recipients, and if so, how many?**

In terms of a threshold for being caught by the legislation the NZBA considers that the Australian approach is preferable to the US model. This would mean that any unsolicited messages would be construed as 'spam' but the penalty would be determined by the extent of the transgression. By specifying little, if any, penalty for low numbers of messages, and allowing an exception for consent to be inferred, the regime would be workable. As the issue of 'bulk' is an important element of genuine spam, the Bank cannot see how this characteristic could be excluded from any anti-Spam legislation.

Again, the Australian experience must be considered, whereby the legislation has classified a 'single electronic message' as spam. This has resulted in significant compliance risks for organisations that have been forced to review all internal and external email messages before they are sent.

The NZBA believes that the definition of 'multiple commercial electronic message' contained in the United State's legislation and other related 'bulk' provisions, should be adopted.

**Q7. Should the messages caught by the legislation be of a commercial advertising and promotional nature only or should other types of messages be caught? Should there be exceptions and if so what should be exempted?**

It is important that certain types of messages are exempt from the scope of any proposed legislation. This is important in the area of service related messages rather than pure sales related messages. It is important for the Banks to be able to contact their customers with technical updates and emergency messages that may affect customers. For example it should be clear that emails from banks to customers warning of danger to their accounts (e.g. phishing) should not be caught.

The Australian experience has highlighted that the definition of Spam is crucial to the success of any anti-Spam legislation. As outlined in paragraph 2 above, the definition of a 'commercial electronic message' adopted by the Australian legislator's is extremely broad and has captured many unintended communications. As a result of the definition, legitimate marketing messages passing between most businesses and their customers, including single electronic messages, are considered spam. The outcome – legitimate business practice has been hindered and many businesses have chosen not to communicate via electronic messages.

**Q8. Should the legislation extend to coverage of acts done overseas? If so, what acts should be covered?**

In a practical sense it may be difficult to provide enforcement against acts done in other jurisdictions, however the NZBA considers that a provision of this sort is in keeping with the policy objectives outlined in paragraph 20, and also in keeping with the necessity for international co-operation to prevent spamming.

**Q9. Should all parties involved in the act of spamming, such as the vendor sponsoring the spamming, be covered by the legislation? Should there be express exceptions such as for telecommunications companies and ISPs?**

(a) All parties involved in the act of spamming should be covered.

(b) The NZBA supports express exceptions for Telco's and ISP's that are subject up to an industry code with specific anti Spam provisions. This way Telco's and ISP's not signed up to an industry code do not receive the benefit of the express exception, and will be subject to anti-Spamming legislation. There should be some protections put in place for domestic users when their systems are hacked by Spammers to send Spam.

**Q10. Should New Zealand adopt an opt-in, double opt-in or opt-out approach in legislating against spam? Why?**

An "express" consent requirement would be too tight, and reasonably inferred consent should be allowed. This would still prevent people "buying a list", but would also allow appropriate judgements based on the individual circumstances. Because of the high potential penalties, if in doubt, marketers will err on the side of caution and seek express or more clearly inferred consent so the commercial incentives will lead to appropriate behaviour.

Requiring "express" consent to particular e-mails may also mean that, in conjunction with high penalties, marketers are overly reluctant to send e-mails, even when it is clear in the circumstances that the customer would like to receive it, but because they have not expressly asked for that e-mail there is doubt as to whether requirements are met. It could be asked "How can someone expressly consent to an e-mail before they have received it and know what it is about?"

**Q11. If an opt-in or double opt-in approach was to be adopted, what should amount to express consent and what actions and/or relationships should amount to inferred consent to the sending of a "commercial" electronic message?**

The Australian approach appears reasonable – if in doubt, the onus is on the marketer to get express or clearly inferred consent otherwise they could face high penalties. Whether consent is express or inferred should be assessed on individual circumstances – firstly by the marketer in deciding whether to send the message, and if necessary in hindsight by the regulator or the courts.

**Q12. How should the scope of any opt-in or double opt-in assent be framed?**

The scope of the opt-in should be whether a particular message was consented to, rather than consenting to e-mails on any subject, or passing details onto other organizations. A wider approach would undermine the purpose of the legislation.

**Q13. Should there be a requirement for commercial electronic messages to accurately identify the sender of the message? If so, what constitutes accurate identification (e.g. name and physical address, name and email address)?**

The NZBA considers that there should be a requirement for accurate and appropriate identification of the sender of messages.

**Q14. Should there be a requirement for commercial electronic messages to include a statement to the effect that the recipient may use an electronic address set out in the message to send an unsubscribe message to the sender, and to ensure that such electronic address is functional?**

See 3<sup>rd</sup> bullet point below under General Comments.

**Q15. Should there be a requirement that commercial electronic messages provide accurate header and subject information?**

Yes, however, the type of information that is required to be accurate would need to be further clarified.

**Q16. Should there be a requirement for the labelling of advertising or adult messages?**

Yes however where a customer has consented to receive information from an organisation, it should be legally able to send that information in such a way that a SPAM filter would not stop it getting through. Otherwise the customer would never receive the requested information because of the labeling requirement.

**Q17. Should anti-Spam legislation include rules against the supply, acquisition and use of address-harvesting software and harvested address lists in connection with the unlawful sending of electronic messages?**

The NZBA considers that removing the “tools” to conduct this would help prevent Spam and would be consistent with the Australian approach of ensuring a comprehensive code against all aspects of a spammer’s activities.

**Q18. Who should be able to bring an action against an alleged spammer?**

An adequately resourced centralized regulatory authority would be the appropriate body to take an action. The NZBA also agrees that giving rights to ISPs might also have merit.

**Q19. What agency should have the enforcement role under the legislation?**

This type of investigative and enforcement activity could be undertaken by the Commerce Commission, so long as it was adequately resourced. Alternatively a new regulatory authority might be established.

**Q20. What should be the available penalties and remedies for breaches of anti-Spam legislation and what should be the maximum fine or pecuniary penalty?**

In order to be effective, and to act as a deterrent, any penalties would have to be significant to avoid spammers making an economic choice to breach the legislation because they considered the economic benefits of advertising outweighed the costs of the penalty. The NZBA considers that additional penalties for continuing breaches as in Australia would also be appropriate.

**Q21. Should contraventions give rise to criminal or civil penalties?**

In general it is desirable that the civil penalty approach is taken. Again, this would be consistent with Australia, and would also benefit from a lower burden of proof (and therefore more likelihood of actions being prosecuted).

**Q22. Should the responsible enforcement agency be given the ability to obtain search warrants conferring powers of entry, search and seizure?**

Yes. See also Q17.

**General Comments**

The NZBA strongly advises MED to consider the Australian banks’ experience with unintended consequences arising from the Australian SPAM Act, to ensure they do not arise in New Zealand legislation.

Particular issues that have arisen for members parent entities in Australia have been:

- The lack of consultation with Banks and the ramifications this has had. The regulator has stated that they did not intend big organisations such as major banks to be caught. The ABA is currently seeking an exemption to the legislation for financial services. Regulators need to weigh up the considerable benefits for customers and businesses being able to do business by email.
- Some of the resulting effects of the SPAM legislation in Australia have meant communication is less consumer friendly as a result of having to manage Spam (e.g. functional unsubscribe).
- Any legislation needs to take into consideration businesses that develop relationships with customers such as banks. This could be reflected in the ability to ask the customer to consent to receive emails at the onset of this relationship therefore doing away with the need for a functional unsubscribe facility. Rather than having a functional unsubscribe facility in an email there would be less of operational impact if the legislation/regulation allowed for reference to such a facility on a website or by calling one number. This reduces the administrative tasks and risk associated with many lists having to be maintained.
- The issue of extra -territoriality needs to be carefully ring-fenced to ensure that it is very clear about what behaviour is to be restricted. One of the unforeseen consequences of the SPAM Act in Australia is due to offshore points having an "Australian link". This means for banks in the Australian jurisdiction emails from Singapore to Beijing have to comply with Australian SPAM legislation.

Yours sincerely



Errol Lizamore  
**Chief Executive**