

From: Ben Creet
Sent: Friday, 12 January 2018 10:34 a.m.
To: Philip van Dyk
Subject: Re: Code of Banking Practice review

Kia ora Philip,

Thank you for meeting with me on Thursday 11 Jan to discuss the Code of Practice and the issues of fraud indemnity.

As discussed - we agree with the position of ConsumerNZ and the Banking Ombudsman and would want to see some form of statement in the Code of Practice that provides a high level confirmation of New Zealand bank's continued commitment to indemnify their customers in relation to card, online banking and Internet fraud.

Additionally, we welcome the commitments that the NZBA's members will be making around confidentiality, privacy and information security. As mentioned, we would like to offer to suggestions on ways that banks should be implementing some of these commitments.

Transparency reporting

The draft Code states "We will respect your privacy and keep your information confidential."

We think that a very important way of providing context and visibility of this respect is for the banks to produce annual transparency reports, setting out the number of times they have been requested or ordered to provide, customer information from government agencies, and the number of times they have complied. TradeMe has been doing transparency reports for a number of years and we have produced some guidance and basic templates for organisations to use when starting to do transparency reports. You can find more information in the links below:

- <https://www.trademe.co.nz/trust-safety/2017/7/25/transparency-2017-1/>
- <https://internetnz.nz/easy-transparency>

Security Vulnerability Disclosure

The draft code states "We will let you know how to report a problem relating to the security of your banking, including any of our electronic banking systems."

We applaud this. Internationally, Coordinated Disclosure is the process that organisations and individuals undertake to ensure that when people find a security vulnerability, they can notify the organisations security team directly, to identify, discuss and fix security vulnerabilities.

We note that currently no major bank in NZ has a coordinated disclosure policy that we could see and we would encourage the NZBA and it's members to implement a Coordinated Disclosure policy as a part of honouring this commitment.

The New Zealand Internet Task Force has written guidelines on Coordinated Disclosure (link below) and here are some links to some other New Zealand organisations Coordinated Disclosure policies, by way of example and a link to the relevant International Standard.

- <http://nzitf.org.nz/coordinated-disclosure/>
- Sky TV: https://skytv.custhelp.com/app/answers/detail/a_id/1797/~/responsible-disclosure-guidelines
- OPC: <https://www.privacy.org.nz/news-and-publications/guidance-resources/vulnerability-disclosure/>
- Vend: <https://www.vendhq.com/nz/responsible-disclosure-policy>
- ISO 29147: <https://www.iso.org/standard/45170.html>

As mentioned - I am available to discuss both transparency reporting and coordinated disclosure policies with you and your members if you want to discuss them further.

Kind regards,

Ben Creet

Issues Manager

InternetNZ

A better world through a better Internet