

[REDACTED]

From: [REDACTED]
Sent: Wednesday, 18 September 2024 11:00 AM
To: Scams Policy
Subject: Scams Prevention Framework – exposure draft legislation

[REDACTED] [REDACTED]
[REDACTED] [REDACTED]

[REDACTED]

Thank you for the opportunity to make a submission in relation to the Scams Prevention Framework, exposure draft legislation; a matter of vital importance to all citizens.

Criminals now rarely rob banks or break into buildings to steal tangible items. They now sit behind computers and/or telephones or facilitate or force others to do so to con businesses and individuals out of their honestly earned money.

I have been the victim of a number of data breaches, where criminals, or so-called malicious actors, have all too easily obtained my personal details from organisations with no or inadequate data security measures and in circumstances where some had no justification for retaining the information as I was not a current customer (and had not been for a lengthy time). I have since received an incessant flow of scam emails, SMS' and attempted telephone calls. Most scam communications are obviously just that, but some are quite sophisticated and one needs to be hyper vigilant. Data breaches aside, criminals are constantly on the hunt for potential victims. When I was a sole trader in the recent past, soon after I commenced business I started to receive scam emails to my business email address, usually fraudulently pretending to be from legitimate sources such as people in government agencies.

Whilst the banks and other financial institutions spin it as choice on the part of consumers, the business model forced upon us by organisations in that sector essentially forces people to manage and transact their finances online. That being so, it is axiomatic that security measures must involve the strongest possible measures available, even if that sometimes means some inconvenience to customers. I find it galling that the banks are collectively acting as knights in shining armour and advertising the fact that they are in the process of implementing security measures they should have introduced many years ago; and they are only doing so because it is obvious they will in due course be forced to (and rightly so). Tech companies which provide email facilities must be forced to 'up their game'. It is, for example, all too simple for criminals to create multiple email addresses in order to bombard potential victims with their malicious communications. It should also be easier for holders of legitimate email accounts to readily block email addresses and it should not be possible for people to either spoof email addresses or to send emails without an email address being displayed.

Operatives in the financial, technological and social media sectors, amongst others, have provided ample opportunity for criminals to operate by utilising their systems and products, under their noses. And whilst they have 'fiddled around the edges' with security, they have not done so in any earnest way because there has been no financial imperative to do so. In fact some businesses, such as social media companies, are seemingly happy to accept advertising revenue from criminals. It is obvious, as Parliaments in other countries have realised is the case for some time, organisations must be forced to both implement a broad suite of measures in an effort to prevent scams and also face the prospect of being forced to compensate

victims of fraud perpetrated with the use of their products and/or technology. And victims should not have to jump through hoops and/or wait unreasonable periods to be compensated. There must be a well-resourced body with unilateral powers to order organisations to pay compensation where either they do not agree to do so upon contact by a customer or their representative, or where the products and/or technology of multiple organisations are involved in the victimisation of someone, and they are finger pointing to seek to apportion blame.

Whilst the proposed legislation does not address this particular issue, it is one that is an important element of the prevention of scams and holding scammers (criminals) to account. Thus, I urge the Government to redouble its interactions with other nation states in order to assist with both scam prevention and multi-jurisdictional criminal investigations; and to provide assistance to third-world nations in this context.

Yours sincerely,

Craig Stevens
Adelaide, South Australia