**Supplementary Submission No. 68.3**
**Inquiry into Cyber Crime**

This is the scenario which played out this morning. Government agencies were alerted, and action has been taken by them. It's unfortunate that while we were able to take that action, the next day, they moved to a compromised machine in France. There is no way to fix this, without the APN.

In the early hours of the morning of the 5th of February, 2010, a hacker sits in his office just within sight of the ** river. His office is in **, a major city, in south eastern ** province of the ** Republic ** of **.

His task this morning is to collect as many pin numbers and account details related to Credit Union members as he possibly can. To start on his task, he creates a dummy web page modelling it on the real Credit Union website, and fashions it in such a way as to place his likely prey at ease.

Next he registers a couple of domain names** . He determines to use an Australian Domain Registry company since that will give it more validity, and he uses contact details and registration information from a location in harmless sounding Sunnyvale, California.

He creates a seemingly harmless email that talks about the bank increasing security to better protect them, warning them, subtly, that they have to fill out this form for them to continue using their account. Logos and fonts belonging to the target Credit Union are used along with those really subtle touches that make it look totally real. But the details they enter don't go to the bank, they are sent to him.

The emails start to leave. They take a circuitous route to ensure increased validity and to further hide their origin. The mail packets head out through Herndon, Virginia, USA using a compromised machine owned by a Communications company. From there, they head out through a mail server which gives them some more validity as they pass through Brussels, Belgium. Leaving there, tens of thousands of messages an hour start heading towards their intended victims in Australia. They pass seamlessly through Spam checkers and anti-viral controls, landing on mailboxes all around the country.

Innocent Credit Union members open the emails. Some of them have read warnings about not opening these emails. Some have not received them at all because their email account is closed or overloaded. Still others are overlooked by users amongst the hundreds of other Spams that have landed in their inbox that morning. But some... some are opened... And have details entered which will allow our Hacker, or more likely his customer or master, to drain funds from accounts all around Australia.

In the early hours of the morning of the 5th of February, 2010, a computer system sits innocuously in a small computer room in Brisbane, Australia. It has detected the email, website, IP addresses and it starts to build a profile of them and compare them to data in its matrix of information built up from the years of experience its had in dealing with these kinds of threats.

Within a short period of time it amasses a sufficient enough collection of data to know that there is a problem and associates it with previous attacks. It identifies the profile of the attackers and notices similarities between this one and one in August of the previous year. It swiftly adds the hostnames and IP Addresses to its collection and marks them as "Phishing activity - Dangerous". System Operators are notified of the threat. And.... How many users in Australia are protected from this threat.

----------------------------------

The Australian Protected Network could have been notified of this threat and protected everyone immediately. There are 710 primary locations where this system _should_ be protecting Australians. Any attempt to access that website or send information to this hacker should be blocked. I'm not saying that we should FORCE every Australian to be on the Australian Protected Network, but we as a society should certainly do everything in our power to encourage them to use it. And that has to start with making it available to them all. The APN is more than just a blocking solution, it's a system developed over as many years as these hackers. And we're ready.

This is not a work of fiction. This scenario has played out today, in this country. And apart from my personally phoning the authorities and telling them, there is little I have the power to do.

Australia needs the Australian Protected Network. My Contact Details are below.

** -- Some Names have been withheld from this document for privacy reasons, or to protect possible ongoing investigations which may, or may not be ongoing within Government agencies based on information provided.

```
-- James :) Collins - Head Office * +61-7-3823-5150 *
  ,-_|\   Web Management InterActive Technologies
 /     *  Sydney Office     - +61-2-8011-3237
 \_,-._/  Canberra Office   - +61-2-6100-7721
      v   Fax Number        - +61-7-3823-5152
www.wmit.net - P.O. Box 1073, Capalaba, Qld, 4157
```