The adequacy of protections for the privacy of Australians online

Submission to Senate Standing Committee of Environment, Communications and the Arts

October 2010

Submitted By:

Trent Youl
Chief Executive Officer
FraudWatch International Pty Ltd

Introduction:

FraudWatch International Pty Ltd (FraudWatch) is making this submission to the Senate Standing Committee of Environment, Communications and the Arts, on The adequacy of protections for the privacy of Australians online, specifically addressing the issue of *"an industry that is protecting the identity of those who own dubious websites,"* which the Senate has expressed interest in learning more about. FraudWatch encounters this particular issue multiple times a day in the services we perform.

FraudWatch is a private, Australian owned, global Internet security company, headquartered in Melbourne. FraudWatch has been operating since 2004, and is one of the few companies in the world that specialise in Anti-Phishing.

Phishing is a technical term for the act of criminals impersonating companies online (mostly financial Institutions), through emails and fake web pages, with the goal of persuading users to provide their personal and financial information (usernames, passwords, login id's, account numbers, credit card numbers etc).

FraudWatch provides "Anti-Phishing" services to companies around the world, monitoring the Internet for emails and web pages impersonating a client's brand. Any company with an online brand is a potential target of phishing. Upon detection of a "phishing" web page, FraudWatch works to have the page taken offline, or shutdown.

A majority of Phishing Web Pages are found on one of two types of websites:

- A newly registered similar to the domain they are impersonating, or
- On a hacked website.

Part of the Phishing Web Page "shutdown" process performed by FraudWatch involves contacting the website owners of hacked websites, to alert them to the fact their site has been compromised, and request their assistance in removing the phishing content from their websites, and fixing the security vulnerabilities which allowed their website to be hacked in the first place.

In order to contact the owners of domains that have been hacked, FraudWatch refers to the WHOIS database, a database listing contact information of the owners of domain names, required to be publically available by ICANN, the international governing body for domain names.

FraudWatch also performs Site Shutdown services on websites that are abusing brands online, not just for phishing, but the misuse of brand logos, brand names, implied association with brands and direct copy of websites.

Some domain registrars now provide a "Domain Privacy Protection" service, where the domain owners contact information is not listed in the WHOIS database, but is replaced by standard contact information for either the domain registrar or the privacy service, making it virtually impossible to actually find, or contact the real owner of the domain.

ICANN Regulations:
(http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm#3)

ICANN, the international governing body for domain names requires that domain registrars make personal contact information of the domain owners publically available.

The following is an excerpt from ICANN's agreement with Domain Registrars, and can be found at http://www.icann.org/en/registrars/ra-agreement-21may09-en.htm#3:

> *3.3 Public Access to Data on Registered Names. During the Term of this Agreement:*
>
> *3.3.1 At its expense, Registrar shall provide an interactive web page and a port 43 Whois service providing free public query-based access to up-to-date (i.e., updated at least daily) data concerning all active Registered Names sponsored by Registrar for each TLD in which it is accredited. The data accessible shall consist of elements that are designated from time to time according to an ICANN adopted specification or policy. Until ICANN otherwise specifies by means of an ICANN adopted specification or policy, this data shall consist of the following elements as contained in Registrar's database:*
>
> *3.3.1.1 The name of the Registered Name;*
>
> *3.3.1.2 The names of the primary nameserver and secondary nameserver(s) for the Registered Name;*
>
> *3.3.1.3 The identity of Registrar (which may be provided through Registrar's website);*
>
> *3.3.1.4 The original creation date of the registration;*
>
> *3.3.1.5 The expiration date of the registration;*
>
> *3.3.1.6 The name and postal address of the Registered Name Holder;*
>
> *3.3.1.7 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the technical contact for the Registered Name; and*
>
> *3.3.1.8 The name, postal address, e-mail address, voice telephone number, and (where available) fax number of the administrative contact for the Registered Name.*

Understanding Privacy Protection Services Offered by Domain Registrars

An increasing number of domain registrars are offering protection of the privacy of domain owners, in the form of a "Privacy Protection Service". This type of service can be commonly referred to as:

- Privacy Protection
- Private Registration
- Domain Privacy
- Proxy Registration
- Whois Privacy Protection

Domain registrars and privacy protection services typically claim the following in relation to the personal contact information within the WHOIS database:

"Everyday, this valuable source of accurate contact information is targeted and harvested by spammers and telemarketers resulting in unwanted and unsolicited contact. Also since your contact information is public, you are at risk for identity theft and fraud and of being contacted by harassers and stalkers."

(http://www.privacyprotect.org/about-privacyprotection/)

Typical benefits claimed by domain registrars provide Domain Registration Privacy Protection Services include:

- To Provide Privacy of the Domain owner,
- To reduce Spam and telemarketers from contacting the domain owner.

An example of how this works is illustrated below, taken from the Privacy Protect Website:

Whilst Domain Privacy protection services often direct you to a web form which apparently allows you to send a message to the domain owner, it has been FraudWatch's experience that these messages do not reach the domain owner.

The Issues of Domain Privacy Protection

Domain Privacy Protection presents a number of issues:

- It is difficult, or in some cases impossible to get in contact with the real domain owners when there is an abuse issue of their website if it has been hacked.
- It allows people to anonymously run websites which may be using dubious business practices, fraud, or theft.
- It allows criminals to hide their contact information and appear to be legitimate - an online haven to remain anonymous.

The Trend of Domain Privacy Protection Services Globally Vs Australian Policy

The trend in the USA for domain registrars to provide Domain Privacy protection has increased greatly in the past 2 years, as registrars see the opportunity the generate revenue from a relatively inexpensive service to provide.

Australian Domains (.com.au, .net.au, .id.au, .org.au, .asn.au) are governed by auDA policy (The Australian Domain Name Administrator). - www.auda.org.au

Specifically, there are 2 policies which govern information provided for the WHOIS database:

Registrant Contact Information Policy (2002-14)

> *Clause 2.2 (part thereof)*
>
> *Registrant Contact - MANDATORY - Contact person or role (eg. "General Manager") nominated by the registrant. In the case of individual registrants, must be the registrant himself or herself. In the case of corporate registrants, must be a principal, employee or member of the registrant.* ***MUST NOT be the registrar of record or their*** **reseller.**

Registrant Contact Information Policy - Clarification of Registrant Contact Information (2008-12)

> *Clause 2.4*
>
> *Registrants* ***must not do anything which may have the effect of concealing the true identity of the registrant or the registrant contact****, unless specifically permitted otherwise by another published policy.*

These policies essentially prohibit the use of Domain Privacy Protection Services concealing the identity of domain registrants for .AU domains.

Although .AU domains are governed by these policies, and do provide transparency about the owners of domains, gTLD domain are not (.com, .net etc). Many Australian Domain registrars provide registration of International Domains which are not covered by auDA policies, to Australians. Some of these Australian domain registrars also provide Domain Privacy Protection Services for non .AU domains.

Conclusion

In the real world. there are regulations which provide some transparency on the public display of company names, proprietors or owners of businesses or associations. The Internet is simply a virtual world, with businesses, associations, information portals and community gathering places. Domains names provide the ability to find the virtual location of these entities online, and WHOIS databases should provide transparent contact information.

Domain Privacy protection services provide no transparency, and whilst intentions of these services may address legitimate privacy concerns of website owners, they allow criminals to hide their identities.

In the interests of Consumer Security and Protection, FraudWatch believes full transparency of the owners of websites should be the standard required within Australia, and would encourage legislation and regulation to ensure this transparency, on ALL domains managed by Australian Registrars, not just .AU domains.