Managing Domain Name Risks

What is Domain Name System Abuse?

Abuses associated with a domain name registration are usually related to IP infringement rights. Many businesses try to protect their "names" by registering multiple domain name variants. This is usually done in order to prevent a third-party registering a name which will trick customers to believe they are doing business with the legitimate corporate entity. It is important to note that DNS monitoring is a weak process and typically only prevents double registrations.

Business Email Compromise (BEC) Fraud is just one example of a fraud scheme that seeks to exploit the weakness in DNS monitoring. For example:

- 'Fraudsters' aim to target a business named "**Corporation Ltd**" and obtain information about the payments they have with a supplier named "**isellstuff**" The supplier uses a domain named "**isellstuff.com**"
- The Fraudsters register a new "look-alike" domain name that resembles that of the supplier, such as: **isellsluff.com**, **isell-stuff.com** (instead of the real '**isellstuff.com**')

What is a Domain Name System?

A Domain Name System (DNS) is the address book of the internet. It allows an internet user to easily search and/or recognize a website or understand the origin of an email. Most internet activity relies on DNS to quickly provide the necessary information to connect users to the IP addresses that they need. DNS translates Internet Protocol (IP) numbers (e.g. 192.193.102.175) into words (e.g. citi.com) and vice versa. Businesses rely on the internet by choosing a Domain Name that will help customers and partners to identify the firm. It usually has two main identifiers:

I. Business name (e.g. **citi**.com)

II. Type of domain (e.g. citi.**com** / citibank.**co.uk**)

What can be done to protect against DNS fraud?

Some steps that can be taken include:

- **Monitor:** Trademark tools and services may be used by firms to monitor potentially fraudulent domain name registration activity
- **Investigate:** Obtaining the registrant's details via a search against a WHOIS* lookup database
- **Report:** Suspicious "look-alike" Domain Names should immediately be reported to the abuse unit of the relevant Domain Registrar(s) which in turn should report to ICANN (Internet Corporation for Assigned Names and Numbers)

*WHOIS is an online tool that allows you to conduct a search and trace the ownership and tenure of a domain name.

GRA30359 04/19