Internet Identity's comments on ICANN's New gTLD Program Explanatory Memorandum regarding Mitigating Malicious Conduct

Rod Rasmussen
President & CTO, Internet Identity

November 22, 2009

I am pleased to provide the following feedback on the issues surrounding the potential for malicious conduct with the expansion of new gTLDs.

This statement is solely on behalf of our company, but is also written with the intent to reflect the interests of our primary customer base: financial institutions and e-commerce companies exposed daily to fraudulent activities perpetuated on the Internet.

In general, we find the nine areas discussed in the memorandum cover many of the top issues we have identified as potential problem areas with the launch of new gTLDs. Some of these issues are truly new, while other recommendations could help keep known issues from getting worse with the launch of hundreds of new TLDs. We find the proposals in the Memorandum to be very good overall, but some are lacking in detail. We look forward to assisting in efforts to better define them. Also, there are some points we believe should be strengthened or extended to cover more than the current memorandum does. We have detailed those below.

Finally, there are some areas that we had hoped to see covered in this memorandum that were not. Our primary concerns in this respect are covered at the end of this response.

Thank you for your consideration of this feedback.

Sincerely,

Rod Rasmussen
President and CEO
Internet Identity
Rod.Rasmussen<at>InternetIdentity.com

Background on Internet Identity and relevance for this response:

Internet Identity is an Internet security company that finds and removes malicious content from the Internet. This includes phishing, malware, fraud and other criminal scams. We work for hundreds of financial companies (banks and credit unions), e-commerce companies, ISPs, domain registrars and registries, online entertainment sites, and many other companies whose customers are victimized by on-line crime. The size of organizations we work for ranges from the very largest on-line properties and banks to small one-branch credit unions and community banks. We participate in numerous organizations and communities that work together to take-on these issues and make the Internet safer and more usable for everyone (except the criminals). These include the Anti-Phishing Working Group (APWG) where I serve as the co-chair of the Internet Policy Committee, the Messaging Anti-Abuse Working Group (MAAWG), the Online Trust Alliance (OTA) where I serve as a Steering Committee member, the Digital Phish-Net alliance between industry and worldwide law enforcement, and the Registry Internet Safety (RISG). We have also been very involved participants in the ICANN process, presenting at numerous ICANN meetings, and participating in various ICANN-related processes and committees exploring the areas where malicious conduct intersects with the ICANN community. None of the statements included in this document should be attributed to any of the organizations to which we belong. They are listed here simply to provide context for the reader as to our level of expertise in this area.

Nine Areas covered in the memorandum

1. Vetted registry operators

Ensuring that criminal organizations and their members do not control or have direct access to registry operations is the most critical issue to cover in the new gTLD launch process. Criminals have already demonstrated the ability to inflict serious damage through bogus "reseller" fronts they have created for registering domain names. It is imperative that we prevent them from running an entire registry, or even placing people within a registry that would allow them unfettered access to create new, theoretically "bullet-proof" domains at will.

We are pleased to see this area covered as the very first issue in the Memorandum. The requirements laid out during the application phase are strong, and should prevent a great deal of mischief. The trademark provisions are superfluous from our point of view, but we can see where they would be helpful in fighting serial cybersquatters, but that is outside the remit of "malicious conduct" in our opinion.

We would like to see the proposal strengthened in two areas to address post-application operations. We are quite concerned that a criminal or abusive organization could stand up a "front" company with "clean" ownership to obtain rights to a registry. After creating this registry, the criminal organization could then take control after the vetting process had finished. A criminal organization could also take over a registry via outright purchase without any subterfuge necessary during the application process. They simply could purchase it later. We anticipate that like in any new, quickly growing market,

some participants, (i.e. new registries) will struggle and face failure. As is common in other industries, that is a time that a criminal organization may step in to take over or "assist" a company in dire straits, and thus gain control.

Short of running a registry, a criminal organization may also attempt to infiltrate one. This is common in many other industries, and we should not think that domain registries, especially in a rapidly growing marketplace, would be immune from this tactic. Recent revelations of fraudulent (and perhaps criminal) behavior by a single individual at the SnapNames domain registration service show that any "bad apple" with access to a domain registration system can do great harm.

Thus we request that the proposed background checks be performed beyond the application period. There are several occasions that could trigger such checks. At the very least, at any point there is a registry ownership change, and at contract renewal. Additional checks could be done at random intervals or when complaints against a registrar indicative of complicity in criminal activities are received. Registries should be contractually bound to comply with such requirements in order for these rules to have any real enforcement power.

Further, registry operators should be required to perform background checks on all key personnel in their employ. This could be accomplished in many ways. For example, using an independent background investigation firm. Results of those checks should be kept on-file, and updated on a regular basis. They should also be auditable by ICANN compliance staff at any time, either via direct communication with the background checking firm, or an escrow system.

2. Demonstrated plan for DNSSEC deployment

Universal deployment of DNSSEC is a critical step needed to close a known security issue that leads directly to "pharming" attacks (DNS cache poisoning). We applaud the inclusion of this strong requirement in the Memorandum. Allowing new registries to start operations without DNSSEC enabled will create new security holes and allow miscreants to target such TLDs. With the root most likely to be signed prior to the launch of any new gTLDs, it makes no sense to allow new gTLDs to publish without signing themselves.

3. Prohibition of wildcarding

We find that this provision has very good merit. There are several security exposures created by wildcard DNS at the TLD level that can be exploited by criminals. There are also a plethora of "unintended consequences" exposures that can lead to inadvertent leakage of confidential information, especially via e-mail when wildcard zones are present for a TLD. Most of these systemic exposures cannot be prevented by organizations put at risk by them, so it is important to keep from increasing the potential for such harms when possible.

4. Removal of orphan glue records when a name server entry is removed from the zone

Internet Identity has been talking about the "orphan glue problem" as an organization for over two years now. We also have been working to support studies and efforts into categorizing this issue. Thus it is no surprise that we enthusiastically support this measure in order to prevent criminals from utilizing "loopholes" in the DNS to help perpetuate their

schemes. Currently, we do not have consistency in operational approaches to handling orphan glue records across the gTLD space, much less the entire TLD space. In many instances this allows criminals to set-up "permanent" nameserver bases for their fraudulent domains. This occurs when the miscreant registers a domain name, creates nameservers using that domain, and then that domain is subsequently suspended without the nameserver entries themselves being removed from the zone file. Such a nameserver delegation becomes a safe haven for setting up new criminal domains, as the nameserver records are guaranteed to resolve until those orphan glue records are removed as well. Establishing a consistent rule for handling such domains in the new gTLDs is an important step towards eliminating this loophole, and providing uniformity for handling all manner of DNS configuration issues across all TLDs.

5. Requirement for thick Whois records

We strongly support this requirement. Lack of consistency of access to whois information can be a significant challenge for law enforcement and first responders. Registries who run thick whois services provide consistent and highly reliable responses. Our experiences with thin registries vary widely, with some registrars that appear to either not have whois properly provisioned, or face repeated systems breakdowns. Keeping whois information in thick format for all new registries will assist our community in tracking down information on miscreant's registration activities. It will also allow us to more readily contact registrants of sites that have been compromised to assist them in securing them.

6. Centralization of zone-file access

We are strong proponents of this measure. First responders, along with many others obtain the daily zone file exports from the current gTLD registries. Running such a system involves a secure operation connecting regularly to all gTLD registries to download and parse large data sets. This is relatively easy to do today given there are just a handful of registry operators. The potential for hundreds of registry operators makes this potentially very difficult to maintain and expensive for most consumers of this data going forward. Centralizing access to the daily zone files, which are already required to be provided anyway, will likely be beneficial to both consumers of zone file data and registries through cost savings and stronger overall security and reliability.

7. Documented registry level abuse contacts and procedures

Yes, absolutely! This provision would likely have the greatest impact on how criminals access and use domains of any of those proposed in the memorandum. We would like to see this provision extended to registrar operators as well. The statement at the end of this section of the memorandum spells this out perfectly:

> *The implementation of new registries, possibly on a large scale, necessitates new, well-defined controls and defined roles in the domain registration process. Abuse contacts and policies at both registry and registrar levels will be a fundamental step in allowing future efforts to combat malicious conduct to continue and scale with the addition of new operators.*

The hard part here is getting the details right, and we stand ready to assist in that process. If implemented well, we believe the domain name industry could make major progress in making the use of domain names far less effective in perpetuating on-line crime.

8. Participation in an Expedited Registry Security Request process

This recommendation is a logical extension of the work already done by ICANN and the existing registries. We support it and see no reason that this would be objectionable to any parties, especially as it is a methodology for a registry operator to obtain contractual relief for large-scale abuses that they help curtail.

9. Draft Framework for High Security Zones Verification

Both our customers and we are staunch supporters of this effort. The response from the American financial industry via various organizations (e.g. BITS, FSTC, etc.) lays out many of these concerns well, and we believe this is a good start for getting the type of necessary security in-place for creating areas of the Internet where consumers can have a high degree of confidence in their safety and transactions. We feel that this type of program should be mandatory for certain types of zones, and extended to industries like healthcare and insurance that have similar issues of privacy and security, as does the financial industry. Beyond that, it would seem to make sense to look at some of the proposed remedies in this area for inclusion for general gTLD security. The argument that you should be safe no matter what corner of the Internet you are exploring is pretty compelling, especially when we are considering policy that could help do just that for some sectors.

Areas left uncovered in the memorandum

Treatment of Domain Name "Resellers"

Our biggest issue that was not covered by the nine points is an accountability and transparency issue. That issue regards the identification, responsibilities, and liabilities of so-called "resellers" of domain registrations. In our opinion, it has yet to be addressed well in the current domain registration space and will likely become an even bigger problem with a large number of new registries. We expect that we will see more resellers as options are expanded with many new registry models. Further, the domain name landscape will become more difficult to navigate for a potential domain registrant, making resellers an important source of advice, as can be seen in other expanding markets. We're likely to see more exploitation through this channel than the already significant amount we see today without better transparency and accountability.

Without better identification of who is providing such services using standards in whois and domain registration contracts, it may be impossible to tell who is responsible for actually handling the domain registration process and who "knows" the registrant. Without definitive accountability as to how registrars must deal with problem resellers or non-responsive ones, it is easy for miscreants to set-up shop under an inattentive registrar. Even with registrars that suspend problem resellers, the ability some registrars offer today for "instant" reseller sign-ups without strict verification of identities allows for miscreants to circumvent many measures designed to keep bad actors from providing domain registration services to criminals.

It is our strong belief that this area needs more attention as part of the new gTLD process.

Capabilities of new registries

The proposed large-scale roll-out of new TLDs could easily lead to unprepared entities being given direct license to create and maintain entire TLDs. From untested legal counsel, to inadequate/inexperienced support staff, to the lack of ability to detect large-scale registrations of abusive domains, there are many potential issues creating attractive venues for criminals to engage in mischief. Past behavior shows that criminals target various ccTLD operators and subdomain resellers to exploit weaknesses in security posture including lack of strong abuse policies and/or technical prowess. New gTLD operators will face similar issues, and those that are not pre-hardened to these tactics may be heavily abused. We would request that provisions be included in the DAG to cover this. For example, all new registries should meet basic operational and training standards in the areas that are exposed to malicious behavior. These functional areas would include at least customer support, network security, legal, and fraud detection.