Annex 6.1

Annexure 6.1 – Dotsecure's application does not create the likelihood of Material Detriment

1. Unprecedented levels of safe-guards in Dotsecure's applications for .bank

Per section 3.5.4 the AGB: "The objector must prove that ***the application*** creates a likelihood of material detriment." The highlighted term – "the application" - is of importance. The likelihood of material detriment must be proven based on the content of the application. IBFed spends 5 pages on trying to prove material detriment, but not once in their arguments do they reference anything from our actual application for .bank.

The Dotsecure application has a significant number of mechanisms built into the application to ensure that only legitimate banks can register general domain names and that there is no abuse in the namespace of .bank. The following are samples of some of the key excerpts from the Dotsecure .bank application:

Question 18 Excerpts:

- Enhance Trust: To create a "trusted and secure" namespace for the banking industry and its users. The .bank extension is intended to provide a .bank registrant an immediately recognized domain name that tells the internet users that they are interacting with a legitimate bank. The .bank TLD will require registrants to achieve specific verification as a bank institute from a recognized authority of national, provincial or state jurisdiction.
- Proxy registrations will not be permitted in .bank
- General domain names in .bank will only be activated after a thorough check against our eligibility criteria, name selection policy and identity verification at the time of registration resulting in a zero abuse namespace at time of registration.
- We will work closely with LEA (Law Enforcement Agencies) and other security groups to mitigate abuse within TLD by providing them with special interfaces (eg searchable whois) and interacting with them regularly in terms of knowledge sharing.
- We follow all of the security specific recommendations in the policy drafted by BITS for financial TLDs. Our description of our implementation of these recommendations is provided in our response to Q24, Q25, Q27, Q28, Q29, Q30, Q40 and Q43.
- .bank implements DNSSEC at the zone which guarantees origin authentication of DNS data, authenticated denial of existence, and data integrity.

Question 28 Excerpts:

- Violation of the following policies will be treated as abuse:

    - Sunrise Policy
    - Trademark Infringement
    - Eligibility Restrictions
    - Name Selection Policy
- Acceptable Usage Policy Violations
    - Intellectual Property, Trademark, Copyright, and Patent Violations including Piracy
    - Spamming
    - Phishing
    - Pharming and DNS Hijacking
    - Distribution of viruses or malware
    - Child pornography
    - Using fast flux techniques
    - Running Botnet command and control operations
    - Hacking
    - Financial and other confidence scams
    - Illegal pharmaceutical distribution
    - Network attacks
    - Violation of applicable laws, government rules and other usage policies

Question 29 Excerpts:

- General Names will be available for registration only to licensed banking institutions
- Each registered general domain name must be similar to the business name, common name, common law name, trademark name, corporate name of the registrant or its product or services or offerings.
- Both of the above criteria along with the identity of the registrant must be validated before a name is activated.
- The above applies to general domain names whether registered during sunrise, landrush or general availability.
- Registration Steps
    - A customer applies to register a domain name
    - Locks are applied to a domain name upon initial registration to prevent any updates
    - The domain is directed to a temporary landing page providing next steps to the Registrant
    - The domain name and the Registrant information is sent to an external agency to validate. The agency validates the domain name against the eligibility requirements policy and name selection policy. The agency also validates the accuracy of the Registrant identity and contact information.
    - Upon successful validation, the locks are removed. A two-factor authentication token (eg RSA SecurID token) is sent to the Registrant securely. The registrant will be able to modify the nameservers of the domain and activate the same.

- Contractual enforcement
    - The following features of Eligibility and name selection policy described above will be executed by the inclusion of corresponding clauses in our RRA, which will require inclusion in registrars' Domain Name Registration Agreements:
        - The registrant must maintain accurate contact information for a domain name
        - The registrant must agree to the Eligibility and name selection policy, and to proceedings under ERDRP
- Anti-phishing Working Group (APWG) review
    - We will work closely with APWG to combat phishing within .bank

The above excerpts from our Dotsecure's .bank application are a few of the anti-abuse, rights protection mechanisms and registration verification policies and procedures that we have committed to use to operate the .bank TLD. We encourage the Panel to review our application in its entirety to gain a clear understanding of the scope and strength of the protections we have outlined. The protections that we have described are inclusive of the BITS recommendations for financial TLDs.

By submitting our application to ICANN, we certified that our statements in our .bank application are accurate and true. The IBFed objection does not evaluate our application based upon those accurate and true statements. Instead, IBFed attempts to utilize sensationalized statistics to smear other legal entities.

We submit that Dotsecure and Directi Internet Solutions are independent companies. While Directi is not the applicant, we have provided a letter from it (Annex 6.3) countering the allegations made by IBFed with the aim of tarnishing its stellar reputation.

Moreover, the fact that IBFed is not part of the Internet industry makes it ignorant about the fact that registrar activities are extremely different from registry activities. Policies such as registration restriction policies are the sole discretion of Registries. The policies detailed by Dotsecure in its capacity as a Registry will be legally enforceable through the Registrars who will be accredited for .Bank. Thus the scope for Abuse in .Bank is not even remotely comparable to abuse to any other unrestricted gTLD.

2. ICANN Eligibility criteria

As part of the Initial Evaluation of applications undertaken by ICANN, any applicant who is not passing the "Applicant Background" criteria of the application is eligible to receive a CQ on the subject from the evaluation panel appointed for the purpose. The Expert Panel should note that none of Radix FZC's 31 subsidiaries has received a single such

question on any of its applications. More specifically, Dotsecure has not received any CQ from ICANN or an evaluation panel with respect to its eligibility or background. Four of Radix's subsidiaries have passed Initial Evaluation. Consequent to this information, we can assure the Expert Panel that Dotsecure has cleared ICANN's background screening, and has been found qualified to run the .Bank registry.

3. Our commitment and ICANN safeguards

Dotsecure is committed to implementing every policy outlined in its application. Our PIC Statement (Annex 6.2) now makes these policies legally enforceable. Dotsecure will negotiate and sign a registry agreement with ICANN that incorporates the application policies into contractual obligations. It is in our best interest to operate a clean namespace that builds trust and secure operations.

The allegation that Dotsecure chose not to file a Community application for .Bank in order to avoid the enforceability of the commitments in the applicant is preposterous. We chose not to do so because we are confident of our assertion that Bank is not a "community" as defined by the AGB.

It is important to note that ICANN has contractual safeguards in the registry agreement for applicants to live up to their commitments. Article 1.3(a)(i) of the registry agreement contains the warranty from the applicant that; "all material information and statements made in the registry TLD application, and statements made in writing during the negotiation of this Agreement, were true and correct at all material respects at the time made, and such information or statements continue to be true and correct in all material respects…."

Furthermore, ICANN has the power under Article 2.11 of the registry agreement to conduct audits twice a year to check on this very point: "to assess compliance by Registry Operator with its representations and warranties contained in Article 1 of this Agreement…." These audits are designed to be extremely thorough; ICANN can visit the Registry premises and demand documentation.

In Article 2.11.c ICANN has the right to increase the frequency of audits to quarterly if the Registry Operator is found, on two consecutive audits: "…not to be in compliance with its representations and warranties contained in Article 1... ICANN has the power to enforce the commitments made in the application. But Article 4.3 is more definitive: ICANN can terminate the contract for failing to cure a"…fundamental and material breach of Registry Operator's representations and warranties set forth in Article 1…"

Lastly, Specification 11 of the Registry Agreement makes the PICs submitted by Dotsecure legally enforceable by incorporation into the Registry Agreement.

4. AGB guidance on proving material detriment

The AGB lays down factors that the panel must use to determine material detriment as follows:

- Nature and extent of damage to the reputation of the community represented by the objector that would result from the applicant's operation of the applied-for gTLD string.
    - There is no evidence of any damage that would result from Dotsecure's operation of .Bank.
    - The security and rights protection measures in Dotsecure's application for .bank are identical to that in fTLD's application, and hence assertions made by IBFed in support of fTLD's application apply to Dotsecure as well.
- Evidence that the applicant is not acting or does not intend to act in accordance with the interests of the community or of users more widely, including evidence that the applicant has not proposed or does not intend to institute effective security protection for user interests.
    - No evidence has been provided by IBFed that Dotsecure intends to act in a manner detrimental to banks.
- Level of certainty that alleged detrimental outcomes would occur.
    - There is no evidence of any detrimental outcomes.
    - IBFed does not provide any arguments to demonstrate any level of certainty that there would be a detrimental outcome, were Dotsecure to be awarded .bank.

Based upon the policies that we have outlined in our application and highlighted above, we assert that Dotsecure's operation of .bank will not result in damage to the reputation of banks globally. Only verified, license-holding banking institutions will be able to register a general .bank domain name.

Annex 6.2

gTLD String: .BANK
Applicant Entity Name: Dotsecure Inc.
Application ID#: 1-1053-59307

SPECIFICATION 11
PUBLIC INTEREST COMMITMENTS

1. Registry Operator will use only ICANN accredited registrars that are party to the Registrar Accreditation Agreement approved by the ICANN Board of Directors on [date to be determined at time of contracting], 2013(or any subsequent form of Registrar Accreditation Agreement approved by the ICANN Board of Directors) in registering domain names. A list of such registrars shall be maintained by ICANN on ICANN's website.

2. ☐Registry Operator will operate the registry for the TLD in compliance with all commitments, statements of intent and business plans stated in the following sections of Registry Operator's application to ICANN for the TLD, which commitments, statements of intent and business plans are hereby incorporated by reference into this Agreement. Registry Operator's obligations pursuant to this paragraph shall be enforceable by ICANN and through the Public Interest Commitment Dispute Resolution Process established by ICANN ((posted at [url to be inserted when final procedure is adopted]), as it may be amended by ICANN from time to time, the "PICDRP"). Registry Operator shall comply with the PICDRP.Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Registry Agreement) following a determination by any PICDRP panel and to be bound by any such determination.

3. ☑Registry Operator agrees to perform following specific public interest commitments, which commitments shall be enforceable by ICANN and through the PICDRP. Registry Operator shall comply with the PICDRP. Registry Operator agrees to implement and adhere to any remedies ICANN imposes (which may include any reasonable remedy, including for the avoidance of doubt, the termination of the Registry Agreement pursuant to Section 4.3(e) of the Registry Agreement) following a determination by any PICDRP panel and to be bound by any such determination.

Dotsecure Inc. respectfully submits the following Public Interest Commitments for the .Bank registry:

1. General Names (as described in section 18b sub-section 4.1 of the application) will be available for registration to licensed banking institutions only.

2. Each registered general domain name must be similar to the business name, common name, common law name, trademark name, corporate name of the registrant or its products or services or offerings.

3. Both of the above criteria along with the identity of the registrant must be validated before a general domain name is activated.

4. The above applies to general domain names whether registered during sunrise, landrush or general availability.

5. Proxy registrations will not be permitted in .Bank.

Annex 6.3

Directi
India: +91.22.3079.7500
US: +1.415.240.4172
Fax. No.: +91.22.3079.7508

9th May 2013

The Expert Panel
ICC International Centre for Expertise
International Chamber of Commerce
38, cours Albert 1er
75008 Paris, France

Subject: EXP/389/ICANN/6 – International Banking Federation vs/ Dotsecure Inc.

Respected Panel,

I am writing to you on behalf of the Directi Group of registrars, against whom certain allegations have been leveled as part of the Community Objection made by the International Banking Federation ("IBFed") against Dotsecure Inc.

1. Introduction to Directi

The Directi Group (www.directi.com) is a 350+ million dollar group of businesses that develop innovative mass-market web products serving millions of customers worldwide. Amongst its businesses are several ICANN accredited registrars, and leading service providers to domain registrars, ISPs, datacenters and Web Hosts. The Directi Group businesses power over 6 million domains worldwide, and have received several accolades for their success in minimizing abusive registrations. Directi's "Zero-Tolerance" procedures and aggressive proactive takedown measures as a domain registrar have resulted in a white-hat reputation.

Mr Bhavin Turakhia, Founder and CEO of Directi currently serves as technical advisor to the local CyberCrime Investigation Cell, and is the former chairman for the Global ICANN Accredited Registrars Constituency for two consecutive terms.

2. IBFed's Allegations regarding the APWG Report

In its objection, the IBFed has used statistics published by the Anti-Phishing Working Group (APWG) in October 2012 as part of their attempt to evidence that the Directi registrars are incompetent at mitigating abusive domain registrations, and that there is a lack of quality

Directi
India: +91.22.3079.7500
US: +1.415.240.4172
Fax. No.: +91.22.3079.7508

control on the front end of Directi's registration process. However, they also admit that the "report does not provide timeliness data (takedown timeframes for Directi for reported phishing domains)". We submit that had IBFed made an attempt to find or analyze this "timeliness data", they would have found that the Directi registrars have amongst the best statistics for mitigating abusive domain registrations.

Furthermore, these statistics in the APWG report are based on registrations in 4 TLDs (.com, .net, .org, and .in), none of whose registry operators have any significant restrictions on domain name registrations. The alleged "lack of quality control on the front end of Directi's registration process" has more to do with the facts that there is a lack of restrictions on registrations (made obligatory only by the registry operator), and that Directi registrars provide amongst the lowest domain registration pricing as part of its business strategy. However, neither of these point to any lack of quality control in Directi's registration process, and its abuse mitigation function.

Lastly, owing to the fact that IBFed is not part of or familiar with the domain registration industry, we submit that they have made allegations without full knowledge of the functioning and regulations of the industry.

Directi's response to the APWG Report

We would like to use this opportunity to provide the Panel with factual details of Directi's efforts related to this APWG report.

Post the publication of the aforementioned report, the abuse team at Directi immediately contacted APWG for additional details regarding the data and methodology used for their report. The APWG team, through IID (Internet Identity) provided us with the list of the 527 abusive domain name registrations via Directi registrars that they had used in order to build their report. An analysis of these domain names revealed the following:

- Directi had received an abuse complaint, and therefore was aware of abuse in only 3 of these 527 domain names. These 3 abusive domains had been suspended prior to the publishing of the report.
- Directi had never been informed / notified regarding the abusive activity in the remaining 524 domains, in spite of IID possessing this data.
- 69% of the abusive registrations had been made via resellers based out of China.
- Over 26% of all the abusive domains had been registered from one single China based reseller.
- 79% of these abusive domain registrations were made in the .IN ccTLD, which is amongst the cheapest available TLDs available in the market. This evidences the fact that low price points lead to these abusive registrations.
- All the abusive registrations were distributed across 4 TLDs (.in, .com, .net, and .org). The registry operators for these 4 TLDs have practically no restrictions on domain registrations in these TLDs.

India: +91.22.3079.7500
US: +1.415.240.4172
Fax. No.: +91.22.3079.7508

- Consequently, registrars such as us have no authority to stop anyone from registering a domain name in any of these 4 TLDs.

Following a thorough analysis of all 527 domains, the following action was taken by Directi:

- All the domain names on the list were suspended within the 48 hour period following the receipt of the report.
- The analysis revealed the identity of all resellers through whom these abusive registrations had taken place. Directi severed business relationships with every reseller who accounted for more than 5 abusive registrations. They accounted for 75% of all domains on the list. Their details are as follows:

Reseller ID	Country	% age of Total Domains Reported
86756	CN	**26.22%**
286299	CN	**7.40%**
328667	CN	**6.77%**
288209	CN	**6.34%**
303190	CN	**4.86%**
271614	CN	**4.23%**
329117	CN	**2.75%**
344474	CN	**2.75%**
146799	US	**2.54%**
253360	CN	**2.11%**
347103	CN	**1.90%**
282235	CN	**1.69%**
285727	IE	**1.69%**
282823	US	**1.27%**
291412	CN	**1.06%**
346125	CN	**1.06%**

- All of the above analysis and corrective action was affected within a 48 hour time frame.

3. IBFed's Allegations regarding Public Domain Registry (PDR)

The IBFed has also alleged that Directi registrars have failed to act in accordance with contractual provisions by not suspending domain names, though they are contractually permitted to do so. They also allege that this has resulted in members of the global banking

Directi
India: +91.22.3079.7500
US: +1.415.240.4172
Fax. No.: +91.22.3079.7508

and financial services sector having to expend financial and legal resources to file UDRP proceedings to combat abusive domain registrations. They have also attached a list of 70 UDRP proceedings involving Directi / Public Domain Registry.

Directi's response regarding PDR

We submit once again that IBFed has made these allegations without full knowledge of the domain registration industry. We would like to provide the Panel with the following information on this subject:

- We acknowledge the fact that Directi registrars / PDR are contractually permitted to suspend abusive domain registrations. However, IBFed has conveniently failed to mention the fact that we are permitted to suspend an abusive domain name only in the event that we are notified of or discover abusive activity in the particular domain name.
- Most industry participants such as domain name lawyers / UDRP focused lawyers are aware of the fact that a simple complaint on the registrars website (such as http://resources.directi.com/report-abuse/), which is free-of-cost will result in an investigation and suspension of the concerned abusive domain name.
- That being said, our experience shows that many corporate lawyers choose to forego this effective mechanism of simply reporting abuse, and instead opt to skip ahead to directly file a costly UDRP case. Perhaps this is because of the greater legal fees associated with a more complicated and expensive procedure.
- An analysis of the 70 UDRP proceedings submitted by the IBFed yields that Directi / PDR was not notified of abuse in a single instance of these cases prior to filing of the UDRP.
- Without any notification or knowledge of abuse in these cases, Directi registrars / PDR were obviously not in a position to take action / suspend these domain names as per its contractual provisions.
- We would once again like to reiterate that these abusive domain names were filed in TLDs such as .com, .net, and .org, all of whose registries do not restrict registrations in their TLD.
- Consequently, no registrar, Directi controlled or otherwise, has the authority to stop anyone from registering a domain name in TLDs that have no restrictions.

4. Directi's work with the Bank of America

Directi recently worked with the Bank of America team to help counter a large scale distributed denial of service (DDoS) Attack against banks. For more background on this case please see

India: +91.22.3079.7500
US: +1.415.240.4172
Fax. No.: +91.22.3079.7508

http://www.informationweek.com/security/attacks/bank-attackers-promise-to-resume-ddos-ta/240144371.

Our work with the Bank of America team led them to provide the following feedback to us:

From email: abuse-reply@bankofamerica.com

"Hi Donesh,

Looks like you are making a ton of headway, only 5 on this list. Thank you so much for knocking these URLs down so quickly. I wish some of the other ISPs on my list were as efficient as your team.

Thnanks again,
Chris"

5. Conclusion

We submit that IBFed's lack of a relationship with and knowledge of the domain registration industry has led it to make these unsubstantiated allegations against Directi and its controlled registrars. We are willing to provide more information / documented evidence of our statements should the Panel / ICANN need it.

We request the Panel to disregard IBFed's claims regarding Directi's incompetence in light of the facts provided in this letter.

Sincerely,

Aman Masjide
Compliance Manager
The Directi Group

Annex 7

Annexure 7 – Evidence of Payment to ICC

Radix FZC (parent entity of Dotsecure Inc.) has made a payment of Euros 5,050 (includes the bank charges) on 9th May 2013 through Emirates Bank in accordance with ICC rules. The confirmation number for the same is **O00009612375**.

Please find the details of the payment below:

```
Message Details
      ***************
      :20:      O00009612375
      :23B:     CRED
      :32A:     130513EUR5050,
      :33B:     AED24821,61
      :36:      4,915170
      :50K:     /AE480260001014331942802
                RADIX FZC
                F19-BC1,RAK FTZ AL MUREED STREET
                P.B. 16113 RAS AL KHAIMAH  UAE
      :56A:     UBSWDEFFXXX
      :57A:     UBSWCHZH80A
      :59:      /CH7900240240224534732
                INTERNATIONAL CHAMBER OF COMMERCE
                38 COURS ALBERT 1 ER 75008 PARIS
                FRANCE
      :70:      FILING FEE CASE REF EXP 389 ICANN 6
                APPLICANT NAME DOTSECURE INC
                DISPUTED STRING BANK APPLICATION
                ID 1 1053 59307
      :71A:     OUR
```

Should any additional details be required, please reach out to us.