GAC Advice Response Form for Applicants

The Governmental Advisory Committee (GAC) has issued advice to the ICANN Board of Directors regarding New gTLD applications. Please see Section IV, Annex I, and Annex II of the GAC Beijing Communique for the full list of advice on individual strings, categories of strings, and strings that may warrant further GAC consideration.

Respondents should use this form to ensure their responses are appropriately tracked and routed to the ICANN Board for their consideration. Complete this form and submit it as an attachment to the ICANN Customer Service Center via your CSC Portal with the Subject, "[Application ID] Response to GAC Advice" (for example "1-111-11111 Response to GAC Advice"). All GAC Advice Responses must be received no later than 23:59:59 UTC on 10-May-2013.

Respondent:

Applicant Name	.Music LLC
Application ID	1-959-51046
Applied for TLD (string)	.Music

Response:

Executive Summary

As a Community applicant for .music, we are confident that we have addressed all of the GAC's concerns in both policy and implementation. By virtue of our decision to file under a "Community" designation and gain the broad support of the music community, we have already committed to enhanced safeguards as part of the contractual oversight of .music. The ICANN board can be assured that our application for .music is fully compliant with not only the Applicant Guidebook, but also the new requirements of the GAC.

The GAC Communique that was issued on April 11th 2013 (hereafter the "GAC Advice"), included four (4) areas which are relevant to our .music application. The GAC:
Area 1- Outlined six safeguards that should apply to ALL new gTLDs and be subject to contractual oversight.
Area 2-. Advised that strings such as .music "invoke a level of implied trust from consumers and carry higher level of risk associated with consumer harm", and therefore should be subject to five (5) additional safeguards, with a further three (3) safeguards possibly applying.
Area 3- (1) Created guidelines for TLDs with restrictive access (our .music application is one), and (2) delared that .music was a generic term, and advised that exclusive access, if implemented, should serve a public interest goal.
Area 4 -Advised the ICANN board that in "those cases where a community, which is clearly impacted by a new set of gTLD applications in contention, has expressed a collective and clear opinion on those applications, such opinions should be duly taken into account, together with all other relevant information.

It is clear that the GAC is looking for more than statements of intent or policy, rather it is looking to ensure all applicants, with particular emphasis on some, have not only adequately planned for the implementation of safeguards against abusive use, but are also contractually held to

account for compliance. To underline this point, and ensure a thorough response, this document will address each of the four areas in detail below.

By way of introduction, .Music LLC., a Far Further company, as a careful, committed and diligent Community applicant for .music, is confident that we have proactively addressed all of the GAC's concerns in both policy and implementation in our original application. By virtue of our decision to file under a "Community" designation, we are already subject to tighter contractual oversight of .music. The ICANN board should be assured that our application for .music is fully compliant with not only the Applicant Guidebook, but also the Advice contained in the GAC's Beijing Communique. Our application for .music is a natural extension of our desire to serve all members of the music community through a trusted namespace that respects creative and Intellectual Property rights. We have invested over six years and substantial resources pursuing this vision and building an unprecedented level of global music community support, which encompasses millions of individual members within more than 1,000 associations in over 150 countries. We respectfully submit that the ICANN Board can have confidence in the strength and thoroughness of our application and resist any calls to delay the program or its progress.

Despite the fact that the .Music LLC. application meets the GAC criteria that are associated with the .music string, we recognize that the GAC document must be discussed in the community before it can be implemented but we hope that the new gTLD process will move forward as planned and not be delayed. We therefore urge the board to withstand requests for any further changes, and or delays.

Area 1: Six safeguards that apply to all new gTLDs

In Annex I, page 7 of the GAC Advice, the GAC identifies six (6) safeguards for for all new gTLD applicants. Each of these is described below, accompanied by our explanation for meeting or exceeding each:
1- Whois verification and checks. We fully meet/exceed this requirement. We have detailed in our response to Q28.4 additional measures we will take on our own initiative to promote Whois accuracy. These measures are exactly what the GAC has requested under this requirement.

2- Mitigating Abuse Activity: We fully meet/exceed this requirement. We define as "abuse" the use of domain names for any of the following activities:
- Spam
- Phishing
- Pharming
- Distribution of malware
- Fast flux hosting
- Botnets
- Distribution of child pornography
- Online sale or distribution of illegal pharmaceuticals.
- Intellectual Property Violation
- Copyright Violation

We have already gone one step further than most applicants, and planned for the implementation of a service that will help detect abusive activity in near real-time, and mitigate it in a consistent and automated manner. We are one of the first adopters of Architelos'

NameSentry Abuse Detection and Mitigation service (www.architelos.com/namesentry). This service, provided by a neutral 3rd party, was specifically designed for the abuse policies and procedures of Far Further's .Music LLC.

3- Security Checks. We fully meet/exceed this requirement. While the GAC's advice here is that registries "periodically" conduct an analysis to see if their domains are being used for abusive purposes, our use of NameSentry ensures that we are ALWAYS scanning our .music TLD to detect any abusive activity within near real-time. The NameSentry service will also automatically match up the abusive domain with the sponsoring registrar and send out a notification asking for resolution of the matter within 12 hours. Since NameSentry will be integrated with our Trouble Ticketing system, a queue will be created for each such instance. If within 12 hours the registrar has not resolved the issue, per our policy we will place the domain on "serverhold". A complete record of every instance will therefore be kept both in our Trouble Ticketing system as well as in NameSentry.

4- Documentation: We fully meet/exceed this requirement. We will perform an audit of a statistical sample of the whois record on an at least twice yearly basis. In addition, our use of NameSentry ensures the availability of an audit trail for every instance of a security threat (due to abuse domain registrations) and our actions. This level of documentation and transparency is unprecedented in current gTLDs, but we believe it demonstrates our commitment to serving our community.

5- Making and handling Complaints: We fully meet/exceed this requirement. As we stated above and in our answer to the Applicant Guidebook Q 28.4 we provide a mechanism for 3rd party complaints about inaccurate Whois. We also will have and publish on our website a single point of contact for complaints related to abuse or illegal use. Lastly, will oversee Registrant Accreditation Criteria and help evaluate enforcement mechanisms, including appeal procedures to ensure the protection of intellectual property rights in the .music TLD.

6- Consequences: We fully meet/exceed this requirement. Our answers to the Applicant Guidebook Q.28 are very clear with regards to consequences for validated breach of the Acceptable Use Policy, providing inaccurate or false Whois data, and other illegal activity. In each of these cases, the sponsoring registrar and its reseller is given 12 hours to investigate the activity further and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety or providing a compelling argument to the registry to keep the name in the zone. If the registrar (reseller) has not taken the requested action after the 12-hour period (i.e., is unresponsive to the request or refuses to take action), the Registry will place the domain on "serverHold".

GAC Area I: Five additional safeguards for TLDs with implied levels of consumer trust

In Annex I, Category 1, of the GAC Advice, the GAC identifies five (5) additional safeguards for a new category of strings including .music. These require:
1- That registry operators include in their Acceptable Use Policy the requirement that registrants comply with all applicable laws.
2- That registrants be notified at the time of registration of the above requirement.

3- That Registry operators will require that registrants who collect and maintain sensitive health and financial data to implement appropriate security measures, as defined by applicable laws and industry standards.
4- That registries establish a working relationship with appropriate regulatory, or industry self-regulatory bodies, including developing a strategy to mitigate risk of fraudulent and illegal activities.
5- That Registry operators require registrants to provide and maintain an up-to-date single point of contact for notifications of complaints or abuse, and for registry operators to maintain in their place of business, the contact details for appropriate regulatory or self-regulating bodies.

The first two requirements are fully met. Far Further's .Music LLC. application specifies that "eligible registrants may register domains in compliance with the Registrant Agreement and its Acceptable Use Policy." In our answer to the Applicant Guidebook's Q.20.e.3, we clearly state that the Registrant Agreement is "presented during the registration process, this agreement will require registrant compliance with the dotMusic Registry rules and Acceptable Use Policy." Our Acceptable Use Policy is reproduced in its entirety in our answer to Q. 28.2 and clearly delineates the types of activities that constitute "abuse" and the repercussions associated with an abusive domain name registration. We also state that this policy is to be incorporated into the Registry-Registrar Agreement, whereby each ICANN-Accredited Registrar must agree to pass through the Acceptable Use Policy to its Resellers (if applicable) and ultimately to the TLD registrants. (Please refer to a copy of our answer attached)

The third requirement is not applicable to .music. The nature of the .music string is different from financial services or health related strings. Our eligibility criteria helps ensure that only members of the music community are allowed to register. These registrants are not likely to collect sensitive health or financial data. We also have specific policies such as Privacy, Data Protection, and even Identity and Access Management amongst others, which are detailed in our answers to Q.30.a.2, of the Applicant Guidebook. (Please refer to a copy of our answer attached)

The fourth requirement is fully met. In our application for .music, we have established various mechanisms for cooperating with appropriate regulatory bodies, as well as the inclusion of a community representative regulatory body, the Policy Advisory Board (PAB). For example, the Acceptable Use Policy may be triggered through a variety of channels to mitigate the risk of fraudulent or illegal activity, including, among other things, community member complaint, private complaint, public alert, government or enforcement agency outreach, and the ongoing monitoring by the Registry or its partners. In all cases, we or our designees will alert Registry's registrar partners about any identified threats, and will work closely with them to bring offending sites into compliance.

The fifth requirement is fully met. Stated another way, this element requires: (a) Whois accuracy, and (b) an additional field in the Whois for capturing registrant contact details for complaints or abuse. With regards to:
(a) we recognize the importance of an accurate, reliable, and up-to-date WHOIS database to governments, law enforcement, intellectual property holders and the public as a whole and are firmly committed to complying with all of the applicable WHOIS specifications for data objects, bulk access, and lookups as defined in Specifications 4 and 10 to the Registry Agreement. In

addition, our Whois Service is compliant with all relevant RFCs including 3912. In addition, we have detailed in our response to the Applicant Guidebook Q28.4 additional measures we will take on our own initiative to promote Whois accuracy. These measures include a mechanism whereby third parties can submit complaints about inaccurate whois directly to the Applicant, as well as a manual review of a random sample of Whois information, no less than twice per year.
(b) our Whois architecture is flexible and has the capability of handling additional fields, such as an abuse point of contact. Regardless of the number of additional fields, the key aim is an accurate Whois database. Our application includes measures well beyond what is contractually required, and should demonstrate our commitment to maintaining an accurate Whois database.
(Please refer to a copy of our answer attached)

AREA 3 - Restricted or exclusive access to a generic gTLD

Restricted acess: Access to .music is governed by a set of eligibilty rules. Potential domain registrants must be members of, or affiliated with, at least one organization in the music community. Domain registrations may be accepted, but will not resolve until the registrant's membership credentials have been verified. This will require verification of relevant membership data during the registration process. This membership will be crosschecked with the relevant member organization. Verification of continued membership is required for renewal, to ensure ongoing eligibility.

Exclusive access: Although the GAC has identified a .music application as one limited by exclusive access, this is a different application than ours. The FarFurther application is open to all those who belong to the community as described in our application.

AREA 4 – Recognizing Community Support

Far Further's .Music LLC. application is currently in contention with seven (7) other applicants. The contending applicants can be categorized as portfolio applicants (Donuts, TLDH, Radix, Famous Four), large Internet companies (Amazon, Google), and another start-up who has chosen to file under a community designation (DotMusic / CGR E-Commerce Ltd).

Prior to submitting our application, we spent years working with representatives from within the worldwide music community to develop policies for creative rights protections and membership requirements that not only serve the common interest of the global music community and meet ICANN's guidelines, but also are balanced with the needs of the internet user and music consumers. In 2011 Far Further's .Music LLC engaged with representative members of the global music community for the opportunity to represent the music community and to submit a .music application on its behalf. After a number of companies, including the other community applicant, went through a thorough vetting process, the community representatives chose to endorse Far Further's .Music LLC. Since then we have continued to receive endorsements from 60 international music-related organizations. These include worldwide music-focused cultural organizations, international musician's unions, music educator's organizations, musical instrument manufacturers, international music distributors, music rights and licensing organizations, independent and major record companies, musicians,

artists, songwriters, music publishers, “DIY” participants and other organizations representing both commercial and non-commercial stakeholders in the music community. For the full list please see http://www.farfurther.com/global-community-support.html

Without question, the music community will be impacted by a .music gTLD. Our mission is to ensure that this is a positive impact by fostering the long term survival and enjoyment of the art in the digital medium by protecting the creative rights of those who make their livelihood from the creation, performance, education and production of music. There is clear and collective support of .Music LLC's application from the music community, as there is no other .music applicant who can claim the number and scale of national and international music organizations as supporters.

SUMMARY

We have spent significant time and resources to proactively meet and in many cases exceed both ICANN’s and even the GAC's expectations of new gTLD applicants. We have designed a registry that is stable and secure, with innovative policies and implementation mechanisms to ensure a safe and secure user experience. We encourage the board to acknowledge the good faith we and many other applicants exercised in believing and participating in the multi-stakeholder process that culminated in the Applicant Guidebook. The process resulted in new protections for communities, consumers and trademark holders. While new recommendations for protections are always welcome, and the .music application addresses these new recommendations, the discussions of these new issues should occur in parallel with application processing. We therefore urge the board to resist delaying the program while new protections are discussed.

20(e). Provide a description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD.

e) Please provide a complete description of the applicant's intended registration policies in support of the community-based purpose of the applied-for gTLD. The .music TLD will be a restricted domain space where second level .music domain names can be registered by eligible individuals, businesses and not-for-profit entities all around the globe. The following policies and mechanisms will be used to ensure support of the community-based purpose of the .music TLD: 1.Music Association/Organization membership: Potential domain registrants must be members of or affiliated with at least one Member Organization of the Global Music Community. Domain registrations may be accepted, but will not resolve until the registrant's membership credentials have been verified. This will require verification of relevant membership data during the registration process. This membership will be crosschecked with the relevant Member Organization. Verification of continued membership is required for renewal, to ensure ongoing eligibility. 2. Registrant Agreement: Presented during the registration process, this agreement will require registrant compliance with the dotMusic Registry rules and Acceptable Use Policy (for details see Q28). 3. Qualified Registrars and Member based Resellers: .music domains will only be available via ICANN accredited registrars (and their resellers) with demonstrated technical capability who have agreed to comply with .music's Registry/Registrar Agreement. In order to ensure strict compliance with .music policy and offer the greatest opportunities to our community, the dotMusic registry will encourage Member Organizations of the GMC to become accredited resellers In addition, .music will operate as a global registry from inception. Formatting flexibility is required to accommodate bandwidth constraints that may be experienced in the developing world. Accordingly, the dotMusic Registry will not mandate any particular formatting or usage. Reserved Names: dotMusic Registry will reserve the following classes of domain names, which will not be available to registrants via the Sunrise or subsequent periods: • The reserved names required in Specification 5 of the new gTLD Registry Agreement. • The geographic names required in Specification 5 of the new gTLD Registry Agreement, and as per our response to Question 21. See our response to Question 22 ("Protection of Geographic Names") for details. • The registry operator will reserve its own name and variations thereof, and registry operations names (such as nic.music, and registry.music,), so that we can point them to our Web site. Reservation of the registry operator's names was standard in ICANN's past gTLD contracts. • We will also reserve names related to ICANN and Internet standards bodies (iana.music, ietf.music, www.music, etc.), for delegation of those names to the relevant organizations upon their request. Reservation of this type of name was standard in ICANN's past gTLD contracts. The list of reserved names will be public prior to the launch of the Sunrise period. Premium Names: • The dotMusic Registry will also designate a set of "premium names," which will be set aside for distribution via special mechanisms. Premium names have been a standard feature of TLD rollouts since 2005. The list of premium names will be public prior to the launch of the Sunrise period. •Premium names will be distributed by application only. Applicants would be required to describe how the intended use of a given premium name will result in demonstrable benefits to the .music community. The policies and procedures for receipt, review, and award of premium name

applications will be based on input from the PAB and will be posted on the dotMusic Registry web site in advance. The rules to ensure transparency, integrity and in the distribution of names, include but are not limited to: a. Strict prohibition of all employees of the dotMusic Registry operator, and its contractors, against bidding in auctions or having any ownership or interest in a premium name applicant. b. Use of the Trademark Clearinghouse during General Availability (Trademark Claims Service) for an additional 60 days, for notifications of new registrations only where the string is a complete match with a filing in the Trademark Clearinghouse. Dispute Resolution Mechanisms: • Registrants and rights holders will have access to several dispute mechanisms. These are fair and transparent processes to adjudicate claims to domain names, and they also protect registrants against reverse domain hijacking. • Names registered in the Sunrise Period will be subject to a Sunrise Dispute Policy. This policy and procedure will be in effect for a finite time period, to provide special protection of qualified trademark rights. Please see our response to Question 29 ("Rights Protection Mechanisms") for full details. • As required by ICANN, .music domains will be subject to the Uniform Dispute Resolution Policy (UDRP). Please see our response to Question 29 ("Rights Protection Mechanisms") for full details. • As required by ICANN, .music domains will also be subject to the Universal Rapid Suspension (URS) policy. Please see our answer to Question 29 ("Rights Protection Mechanisms") for full details. • We will provision systems to take in and administrate cases as per ICANN's Registrar Transfer Dispute Resolutions Policy (http://www.icann.org/en/transfers/dispute-policy-12jul04.htm). This process will allow registrars to protect registrants by filing disputes about inter-registrar transfers that they believe were unauthorized or improperly executed. • MEDRP: .music will support the Music Eligibility Dispute Resolution Procedure. This dispute mechanism will be available to members of the .music community and end-users to file claims against registrants of the .music domain for violations of the .music eligibility and use community rules and policies. We will select an adjudication service from the list of ICANN approved arbitrators to facilitate MEDRP claims (please see Q28 and Q29 for further details). Eligibility: who is eligible to register a second-level name in the gTLD, and how will eligibility be determined. - Potential domain registrants must be members of or affiliated with at least one Member Organizations of the Global Music Community. Domain registrations may be accepted, but will not resolve until the registrant's membership credentials have been verified. Please see the "Proposed .music Registration Process" attachment in our answer to Q48 for a step-by-step visual depiction of the process. Should the registrant fail to meet the eligibility criteria, they risk the suspension and ultimately deletion or loss of their domain name. Verification of continued membership is required for renewal, to ensure ongoing eligibility. Name selection: what types of second-level names may be registered in the gTLD. - Please see the Reserve Name policy detailed above. Beyond these, eligible registrants may register domains in compliance with the Registrant Agreement and its Acceptable Use Policy. Content/Use: what restrictions, if any, the registry operator will impose on how a registrant may use its registered name. - Registrants must hold valid rights to all materials displayed on and/or distributed through their specific site. Please see Q28 for details on .music's Acceptable Use Policy. The dotMusic registry will be regularly monitored potential violations and also provide a robust abuse reporting process for such violations noticed by others. Should the

registrant be found in violation, they risk the suspension and ultimately deletion or loss of their domain name. Enforcement: what investigation practices and mechanisms exist to enforce the policies above, what resources are allocated for enforcement, and what appeal mechanisms are available to registrants. - The .music Registry-Registrar and the Registrant Agreements will include extensive monitoring, enforcement (up to and including take downs) as well as appeal provisions. Monitoring o The .music TLD will be monitored by online scanning tools such as those that search for keywords that are commonly used to identify the availability of music distributed without appropriate authorization or in violation of intellectual property rights. Suspected abuse from such automated search tools will flag an analyst from our abuse team (see Q28) who will then access and review the website to confirm the abuse. Neustar will enable .music analysts to suspend domain names as required. o The dotMusic Registry will also use Abuse Mitigation Services to monitor, detect and mitigate domain name abuses (se Q29) Enforcement and Appeal o Registrants in violation of the Registrant Agreement risk the suspension and ultimately deletion or loss of their domain name. o As detailed in our answer to Q28, failure to comply with the Registry-Registrar agreement will result in loss or revocation of registrar accreditation. o The dotMusic Registry will use standard dispute mechanisms (see Q28 and Q29), such as UDRP, URS etc. However, in the case of serious allegations of failure to meet community member eligibility requirements, we have created a MEDRP (Music Community Eligibility Dispute Resolution Procedure). This dispute mechanism will be arbitrated by a third party approved by ICANN such as WIPO and will be binding on all parties (provisions will be named in the Registrant Agreement). Disputes may be initiated by community members or end-users; however, there will be reasonable limitations developed on the filing of disputes to prevent abuse of the mechanism. Please see our answer to Q20(b) under "Accountability mechanisms of the applicant to the community" for additional details on appeal procedures.

28. Abuse Prevention and Mitigation

28.1 Abuse Prevention and Mitigation

Strong abuse prevention of a new gTLD is an important benefit to the internet community. .music and its registry operator and back-end registry services provider, Neustar, agree that a registry must not only aim for the highest standards of technical and operational competence, but also needs to act as a steward of the space on behalf of the Internet community and ICANN in promoting the public interest. Neustar brings extensive experience establishing and implementing registration policies. This experience will be leveraged to help .music combat abusive and malicious domain activity within the new gTLD space.

One of those public interest functions for a responsible domain name registry includes working towards the eradication of abusive domain name registrations, including, but not limited to, those resulting from:

- Illegal or fraudulent actions
- Spam
- Phishing

- Pharming
- Distribution of malware
- Fast flux hosting
- Botnets
- Distribution of child pornography
- Online sale or distribution of illegal pharmaceuticals.
- Intellectual Property Violation
- Copyright Violation

More specifically, although traditionally botnets have used Internet Relay Chat (IRC) servers to control registry and the compromised PCs, or bots, for DDoS attacks and the theft of personal information, an increasingly popular technique, known as fast-flux DNS, allows botnets to use a multitude of servers to hide a key host or to create a highly-available control network. This ability to shift the attacker's infrastructure over a multitude of servers in various countries creates an obstacle for law enforcement and security researchers to mitigate the effects of these botnets. But a point of weakness in this scheme is its dependence on DNS for its translation services. By taking an active role in researching and monitoring these sorts of botnets, .music's partner, Neustar, has developed the ability to efficiently work with various law enforcement and security communities to begin a new phase of mitigation of these types of threats.

Policies and Procedures to Minimize Abusive Registrations

A Registry must have the policies, resources, personnel, and expertise in place to combat such abusive DNS practices. As .music's registry provider, Neustar is at the forefront of the prevention of such abusive practices and is one of the few registry operators to have actually developed and implemented an active "domain takedown" policy. We also believe that a strong program is essential given that registrants have a reasonable expectation that they are in control of the data associated with their domains, especially its presence in the DNS zone. Because domain names are sometimes used as a mechanism to enable various illegitimate activities on the Internet often the best preventative measure to thwart these attacks is to remove the names completely from the DNS before they can impart harm, not only to the domain name registrant, but also to millions of unsuspecting Internet users.

Removing the domain name from the zone has the effect of shutting down all activity associated with the domain name, including the use of all websites and e-mail. The use of this technique should not be entered into lightly. .music has an extensive, defined, and documented process for taking the necessary action of removing a domain from the zone when its presence in the zone poses a threat to the security and stability of the infrastructure of the Internet or the registry.

Abuse Point of Contact

As required by the Registry Agreement, .music will establish and publish on its website a single abuse point of contact responsible for addressing inquiries from law enforcement, its community members and the public related to malicious and abusive conduct. .music will also provide such information to ICANN prior to the delegation of any domain names in the TLD. This information shall consist of, at a minimum, a valid e-mail address dedicated solely to the handling of malicious

conduct complaints, and a telephone number and mailing address for the primary contact. We will ensure that this information will be kept accurate and up to date and will be provided to ICANN if and when changes are made. In addition, with respect to inquiries from ICANN-Accredited registrars, our registry services provider, Neustar, shall have an additional point of contact, as it does today, handling requests by registrars related to abusive domain name practices.

28.2 Policies Regarding Abuse Complaints

One of the key policies each new gTLD registry will need to have is an Acceptable Use Policy that clearly delineates the types of activities that constitute "abuse" and the repercussions associated with an abusive domain name registration. In addition, the policy will be incorporated into the applicable Registry-Registrar Agreement and reserve the right for the registry to take the appropriate actions based on the type of abuse. This will include locking down the domain name - preventing any changes to the contact and nameserver information associated with the domain name, placing the domain name "on hold" rendering the domain name non-resolvable, transferring to the domain name to another registrar, and/or in cases in which the domain name is associated with an existing law enforcement investigation, substituting name servers to collect information about the DNS queries to assist the investigation.

The dotMusic Registry will adopt an Acceptable Use Policy that clearly defines the types of activities that will not be permitted in the TLD and reserves the right of the Applicant to lock, cancel, transfer or otherwise suspend or take down domain names violating the Acceptable Use Policy and allow the Registry where and when appropriate to share information with law enforcement. Each ICANN-Accredited Registrar (even in the case of a sole registrar model) must agree to pass through the Acceptable Use Policy to its Resellers (if applicable) and ultimately to the TLD registrants. Below is the Registry's initial Acceptable Use Policy that we will use in connection with .music.

the dotMusic Registry Acceptable Use Policy

This Acceptable Use Policy gives the Registry the ability to quickly lock, cancel, transfer or take ownership of any .music domain name, either temporarily or permanently, if the domain name is being used in a manner that appears to threaten the stability, integrity or security of the Registry, or any of its registrar partners – and/or that may put the safety and security of any registrant or user at risk. The process also allows the Registry to take preventive measures to avoid any such criminal or security threats.

The Acceptable Use Policy may be triggered through a variety of channels, including, among other things, community member complaint, private complaint, public alert, government or enforcement agency outreach, and the on-going monitoring by the Registry or its partners. In all cases, the Registry or its designees will alert Registry's registrar partners about any identified threats, and will work closely with them to bring offending sites into compliance.

The following are some (but not all) activities that will be subject to rapid domain compliance:

- Phishing: the attempt to acquire personally identifiable information by masquerading as a website other than .music's own.
- Pharming: the redirection of Internet users to websites other than those the user intends to visit, usually through unauthorized changes to the Hosts file on a victim's computer or DNS records in DNS servers.
- Dissemination of Malware: the intentional creation and distribution of "malicious" software designed to infiltrate a computer system without the owner's consent, including, without limitation, computer viruses, worms, key loggers, and Trojans.
- Fast Flux Hosting: a technique used to shelter Phishing, Pharming and Malware sites and networks from detection and to frustrate methods employed to defend against such practices, whereby the IP address associated with fraudulent websites are changed rapidly so as to make the true location of the sites difficult to find.
- Botnetting: the development and use of a command, agent, motor, service, or software which is implemented: (1) to remotely control the computer or computer system of an Internet user without their knowledge or consent, (2) to generate direct denial of service (DDOS) attacks.
- Malicious Hacking: the attempt to gain unauthorized access (or exceed the level of authorized access) to a computer, information system, user account or profile, database, or security system.
- Child Pornography: the storage, publication, display and/or dissemination of pornographic materials depicting individuals under the age of majority in the relevant jurisdiction.
- Community Abuse Considerations: The dotMusic Registry will create a safe TLD in .music by actively monitoring and and combating copyright infringement, cybersquatting, typo-squatting and any other domain name and registration based abusive practices. They will also actively monitor and combat the harder abuse instances that plague the music industry in the online world. These are defined as copyright infringement that results from P2P sharing, illegal digital distribution, along with any and all types of Intellectual Property infringement involving the DNS.

The Registry reserves the right, in its sole discretion, to take any administrative and operational actions necessary, including the use of computer forensics and information security technological services, among other things, in order to implement the Acceptable Use Policy. In addition, the Registry reserves the right to deny, cancel or transfer any registration or transaction, or place any domain name(s) on registry lock, hold or similar status, that it deems necessary, in its discretion; (1) to protect the integrity and stability of the registry; (2) to enforce the requirements of community membership and acceptable use (3) to comply with any applicable laws, government rules or requirements, requests of law enforcement, or any dispute resolution process; (4) to avoid any liability, civil or criminal, on the part of Registry as well as its affiliates, subsidiaries, officers, directors, and employees; (5) per the terms of the registration agreement or (6) to correct mistakes made by the Registry or any Registrar in connection with a domain name registration. Registry also reserves the right to place upon registry lock, hold or similar status a domain name during resolution of a dispute.

Taking Action Against Abusive and/or Malicious Activity

The Registry is committed to ensuring that those domain names associated with abuse or Malicious conduct in violation of the

Acceptable Use Policy are dealt with in a timely and decisive manner. These include taking action against those domain names that are being used to threaten the stability and security, the community requirements of the TLD, or is part of a real-time investigation by law enforcement.

Once a complaint is received from a trusted source, third-party, or detected by the Registry, the Registry will use commercially reasonable efforts to verify the information in the complaint. If that information can be verified to the best of the ability of the Registry, the sponsoring registrar and the relevant reseller will be notified and be given 12 hours to investigate the activity and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety or providing a compelling argument to the Registry to keep the name in the zone. If the registrar (reseller) has not taken the requested action after the 12-hour period (i.e., is unresponsive to the request or refuses to take action), the Registry will place the domain on “ServerHold”. Although this action removes the domain name from the TLD zone, the domain name record still appears in the TLD WHOIS database so that the name and entities can be investigated by law enforcement should they desire to get involved.
Coordination with Law Enforcement

With the assistance of Neustar as its back-end registry services provider, .music can meet its obligations under Section 2.8 of the Registry Agreement where required to take reasonable steps to investigate and respond to reports from law enforcement and governmental and quasi-governmental agencies of illegal conduct in connection with the use of its TLD. The Registry will respond to legitimate law enforcement inquiries within one business day from receiving the request. Such response shall include, at a minimum, an acknowledgement of receipt of the request, Questions or comments concerning the request, and an outline of the next steps to be taken by .Music for rapid resolution of the request.

In the event such request involves any of the activities which can be validated by the Registry and involves the type of activity set forth in the Acceptable Use Policy, the sponsoring registrar and its reseller is then given 12 hours to investigate the activity further and either take down the domain name by placing the domain name on hold or by deleting the domain name in its entirety or providing a compelling argument to the registry to keep the name in the zone. If the registrar (reseller) has not taken the requested action after the 12-hour period (i.e., is unresponsive to the request or refuses to take action), the Registry will place the domain on “serverHold”.

Monitoring for Malicious Activity

28.3 Measures for Removal of Orphan Glue Records

As the Security and Stability Advisory Committee of ICANN (SSAC) rightly acknowledges, although orphaned glue records may be used for abusive or malicious purposes, the “dominant use of orphaned glue supports the correct and ordinary operation of the DNS.” See http://www.icann.org/en/committees/security/sac048.pdf.

While orphan glue often support correct and ordinary operation of the DNS, we understand that such glue records can be used maliciously to point to name servers that host domains used in illegal phishing, bot-

nets, malware, and other abusive behaviors. Problems occur when the parent domain of the glue record is deleted but its children glue records still remain in DNS. Therefore, when the Registry has written evidence of actual abuse of orphaned glue, the Registry will take action to remove those records from the zone to mitigate such malicious conduct.

Neustar run a daily audit of entries in its DNS systems and compares those with its provisioning system. This serves as an umbrella protection to make sure that items in the DNS zone are valid. Any DNS record that shows up in the DNS zone but not in the provisioning system will be flagged for investigation and removed if necessary. This daily DNS audit serves to not only prevent orphaned hosts but also other records that should not be in the zone.

In addition, if either .music or Neustar become aware of actual abuse on orphaned glue after receiving written notification by a third party through its Abuse Contact or through its customer support, such glue records will be removed from the zone.

28.4 Measures to Promote WHOIS Accuracy

The dotMusic Registry acknowledges that ICANN has developed a number of mechanisms over the past decade that are intended to address the issue of inaccurate WHOIS information. Such measures alone have not proven to be sufficient and .music will offer a mechanism whereby third parties can submit complaints directly to the Applicant (as opposed to ICANN or the sponsoring Registrar) about inaccurate or incomplete WHOIS data. Such information shall be forwarded to the sponsoring Registrar, who shall be required to address those complaints with their registrants. Thirty days after forwarding the complaint to the registrar, .music will examine the current WHOIS data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or there was some other disposition. If the Registrar has failed to take any action, or it is clear that the Registrant was either unwilling or unable to correct the inaccuracies, Applicant reserves the right to suspend the applicable domain name(s) until such time as the Registrant is able to cure the deficiencies.

In addition, .music shall on its own initiative, no less than twice per year, perform a manual review of a random sampling of .music domain names to test the accuracy of the WHOIS information. Although this will not include verifying the actual information in the WHOIS record, .music will be examining the WHOIS data for prima facie evidence of inaccuracies. In the event that such evidence exists, it shall be forwarded to the sponsoring Registrar, who shall be required to address those complaints with their registrants. Thirty days after forwarding the complaint to the registrar, the Applicant will examine the current WHOIS data for names that were alleged to be inaccurate to determine if the information was corrected, the domain name was deleted, or there was some other disposition. If the Registrar has failed to take any action, or it is clear that the Registrant was either unwilling or unable to correct the inaccuracies, .music reserves the right to suspend the applicable domain name(s) until such time as the Registrant is able to cure the deficiencies.

28.4.1 Authentication of Registrant Information and Monitoring of

Registration Data

Authentication of registrant information as complete and accurate at time of registration. Most .music registrations will be sold by “reseller”.music community member associations to their memberships. These resellers will in many cases be able to verify their own memberships at the time of domain sale. To address the case where the reseller lacks the ability to do this in the domain sale process, the .music reseller platform will capture all registrant declaration as to community membership including the identification of their accredited member association. All registrations associated with a given member association will be reported daily to the relevant member association for asynchronous review. Discrepancies in declared community membership will be addressed through the standard abuse practices described in the Acceptable Use Policy.

28.4.3 Policies and Procedures Ensuring Compliance (RRA and RA)

The dotMusic Registry intends to operate as a sole registrar model but will offer exclusive reseller services for music associations to sell domain names to their memberships. This registrar entity and subsequent resellers will be required to enforce measures, establish policies and procedures to ensure compliance, which may include audits, financial incentives, penalties, or other means.

The Registry-Registrar Agreement (RRA) will contain the following terms which will be passed through to the Reseller Agreements where applicable:

1. Confirming that Registrants have a bona fide affiliation with a legitimate Community Member.
2. Requiring that Registrants execute a Registrant Agreement which provides an additional level in securing the protection of creative and intellectual property rights and serves to mitigate copyright infringement, piracy and any other abuse as outlined in the dotMusic Registry policies.
   a. The electronic acceptance of the Registrant Agreement would be a pre-requisite to the confirmation of any registration or renewal transaction performed by the Registrar (reseller).
   b. Ensuring an electronic audit trail is maintained at the registrar, referencing each and every .music registration to an acceptance date of the Registrant Agreement.
3. Requiring their registrants to certify on an annual basis that they are in compliance with all Accreditation Criteria and other policies and requirements governing domains, including, but not limited to, that the registrant:
   a. is not, and will not be involved in any form of copyright infringement, or otherwise facilitate such copyright infringement or provide access to any software, service or application that facilitates copyright infringement, directly or indirectly through the domain;
   b. has all the rights necessary to transmit, display, provide access to, reproduce, distribute, publish, link to, perform or otherwise exploit any copyrighted content made available directly or indirectly through the domain;
   c. has and will maintain appropriate records sufficient to verify any claimed licenses or authorizations to use or exploit creative content owned by third parties;
   d. will only use the domain in connection with activities involving

legitimate/authorized uses of creative works and not to facilitate infringement; and

e. meets the other Accreditation Criteria and that their operation of the site is legal

4. Acknowledgement that proxy registrations are disallowed, except those proxy registration services that are approved by, and fully comply with ICANN standards and .Music Registry policies.

5. Acknowledgement that the registrar and/or reseller will enforce the terms of the Registrant Agreement.

6. Acknowledgement that the registrar and/or reseller will endeavor to maintain WHOIS accuracy by:

a. authenticating the registrant information as complete and accurate at time of registration,

b. ensure the registrant is a valid member of good standing in at least of one of Coalition Member Organizations. Means requiring submission of identifying membership information.

c. ensuring completeness and verifying all contact information of principals mentioned in registration data. Means may include utilizing simple web based technology to discern and thus reject inaccurate data (such as mismatch of zip code and State Code), and other means,

d. regular monitoring of registration data for accuracy and completeness, employing authentication methods, and establishing policies and procedures to address domain names with inaccurate or incomplete WHOIS data. Means to do so would include periodic email alerts to the domain name registrant to verify or correct WHOIS information.

7. Acknowledgement of and compliance with .Music Registry's abuse detection and mitigation procedures, up to and including domain takedown.

8. Acknowledgement of the .Music Registry's right to take action to ensure compliance with the abuse detection and mitigation policies and procedures of the .Music Registry.

a. Acceptance of .Music's right to suspend domains found to be in violation of .Music policies.

b. Implement reasonable procedures to identify repeat registrants that attempt to avoid detection as repeat offender registrants, etc.

c. Registrar (resellers) will be required to promptly take down/deregister domains that fail to comply with the Accreditation Criteria and other policies governing domains (including, but not limited to breach of the certification contemplated below), and to refuse to accept registrations from registrants that previously violated such criteria or policies.

d. Annual verification of and electronic acceptance of the RRA.

Last but not least, the .Music Registry will create the Registrant Agreement. The RA would be furnished to all .Music registrar's resellers as part of the reseller accreditation procedures. The RA would at a minimum require all registrants to:

1. Agree to and abide by the terms of the .Music Registrant Agreement.

2. Adhere to the protection of Creative and Intellectual Property rights such as mitigating copyright infringement and piracy as well as guarding against other abuses such as cyber squatting, typo-squatting or other abusive registration practices defined in the agreement.

3. Annually notifying Registrants of their current agreement to:

a. Avoid of any form of copyright infringement, or otherwise facilitate such copyright infringement or provide access to any

software, service or application that facilitates copyright infringement, directly or indirectly through the domain;
b. Possess all necessary rights to transmit, display, provide access to, reproduce, distribute, publish, link to, perform or otherwise exploit any copyrighted content made available directly or indirectly through the domain;
c. Maintain appropriate records to sufficiently verify any claimed licenses or authorizations to use or exploit creative content owned by third parties;
d. Use the domain only in connection with activities involving legitimate/authorized uses of creative works and not to facilitate infringement;
e. Meet other Accreditation Criteria as set forth from time to time
f. Implement reasonable monitoring of their site and their domain to police against infringing activity;
g. Implement reasonable enforcement procedures to ensure that any unauthorized content isremoved before being placed on the domain or immediately removed once the registrant becomes aware of such unauthorized content;
h. Proactively ensure unauthorized content is not made available via the domain;
i. Acknowledge the .Music Registry's right to engage in monitoring and policing activity of the registrant's domain and site; and
j. Provide evidence of reasonable security and other measures that will be used to protect content made available from the domain.
4. Acknowledgement that if the registrant's domain use is found to be in violation of the .Music Registrant Agreement, the domain will be subject to suspension and reclaimed by the Registry.

.Music Registry will set itself up as a sole registrar, providing reseller capability to Community Member Associations, who will in turn sell .Music domains to their memberships. This model will provide the following advantages:

- minimize malicious conduct in .music (eg: quicker takedown in case of abusive behavior),
- minimize dot Music Registry's administrative and technical costs,
- maximize compliance with dotMusic Registry policies, and
- maximize control, as the dotMusic Registry would be the "Registrar of Record" in the WHOIS.

28.5 Resourcing Plans

Responsibility for abuse mitigation rests with a variety of functional groups. The Abuse Monitoring team is primarily responsible for providing analysis and conducting investigations of reports of abuse. The customer service team also plays an important role in assisting with the investigations, responded to customers, and notifying registrars of abusive domains. Finally, the Policy/Legal team is responsible for developing the relevant policies and procedures.

The necessary resources will be pulled from the pool of available resources described in detail in the response to Question 31, as well as resources described under the Abuse and Compliance Team. The following resources are available from those teams:

Customer Support – 12 employees

Policy⁄Legal – 2 employees
Abuse and Compliance Monitoring Team – 4 employees

The dotMusic Registry, as noted in our financials, has provisioned for a community compliance and support function. Oncall 24⁄7⁄365, this team supports both the community eligibility verification functions as well as providing a Tier 2 escalation for abuse cases reported through the Tier 1 Neustar Customer Support Teams. We estimate the community and compliance support function will spend no more than 10% of their collective time responding to abuse complaints in view of the estimated registration volumes and for the following reasons:

– Registrants are verified members of an accredited .music community organization or association in order to have an "active" registration and are held to strict community eligibility requirements
– Registrants are well informed that IP protection is a fundamental priority to attain a .music domain. They risk substantial investment loss by risking non-compliance to the participation requirements in .music
– Registrants who lose their .music registrations due to non-compliance can put their related music organization or association memberships at risk
– The .music domain while market-competitive, is not a low cost domain space, which further has a cooling effect on attempted abusive registration
– Regular compliance scanning of the namespace for both community eligibility requirement conformance and abuse detection, as described in Q18 and earlier in Q28 will operate as a deterrent to abusive registration use.

30.(a).2 Summary of Security Policies

Neustar has developed a comprehensive Information Security Program in order to create effective administrative, technical, and physical safeguards for the protection of its information assets, and to comply with Neustar's obligations under applicable law, regulations, and contracts. This Program establishes Neustar's policies for accessing, collecting, storing, using, transmitting, and protecting electronic, paper, and other records containing sensitive information.

-The policies for internal users and our clients to ensure the safe, organized and fair use of information resources.

-The rights that can be expected with that use.

-The standards that must be met to effectively comply with policy.

-The responsibilities of the owners, maintainers, and users of Neustar's information resources.

-Rules and principles used at Neustar to approach information security issues

The following policies are included in the Program:

1. Acceptable Use Policy

The Acceptable Use Policy provides the rules of behavior covering all Neustar Associates for using Neustar resources or accessing sensitive information.

2. Information Risk Management Policy

The Information Risk Management Policy describes the requirements for the on-going information security risk management program, including defining roles and responsibilities for conducting and evaluating risk assessments, assessments of technologies used to provide information security and monitoring procedures used to measure policy compliance.

3. Data Protection Policy

The Data Protection Policy provides the requirements for creating, storing, transmitting, disclosing, and disposing of sensitive information, including data classification and labeling requirements, the requirements for data retention. Encryption and related technologies such as digital certificates are also covered under this policy.

4. Third Party Policy

The Third Party Policy provides the requirements for handling service provider contracts, including specifically the vetting process, required contract reviews, and on-going monitoring of service providers for policy compliance.

5. Security Awareness and Training Policy

The Security Awareness and Training Policy provide the requirements for managing the on-going awareness and training program at Neustar. This includes awareness and training activities provided to all Neustar Associates.

6. Incident Response Policy

The Incident Response Policy provides the requirements for reacting to reports of potential security policy violations. This policy defines the necessary steps for identifying and reporting security incidents, remediation of problems, and conducting lessons learned post-mortem reviews in order to provide feedback on the effectiveness of this Program. Additionally, this policy contains the requirement for reporting data security breaches to the appropriate authorities and to the public, as required by law, contractual requirements, or regulatory bodies.

7. Physical and Environmental Controls Policy

The Physical and Environment Controls Policy provides the requirements for securely storing sensitive information and the supporting information technology equipment and infrastructure. This policy includes details on the storage of paper records as well as access to computer systems and equipment locations by authorized personnel and visitors.

8. Privacy Policy

Neustar supports the right to privacy, including the rights of individuals to control the dissemination and use of personal data that describes them, their personal choices, or life experiences. Neustar supports domestic and international laws and regulations that seek to protect the privacy rights of such individuals.

9. Identity and Access Management Policy

The Identity and Access Management Policy covers user accounts (login ID naming convention, assignment, authoritative source) as well as ID lifecycle (request, approval, creation, use, suspension, deletion, review), including provisions for system/application accounts, shared/group accounts, guest/public accounts, temporary/emergency accounts, administrative access, and remote access. This policy also includes the user password policy requirements.

10. Network Security Policy

The Network Security Policy covers aspects of Neustar network infrastructure and the technical controls in place to prevent and detect security policy violations.

11. Platform Security Policy

The Platform Security Policy covers the requirements for configuration management of servers, shared systems, applications, databases, middle-ware, and desktops and laptops owned or operated by Neustar Associates.

12. Mobile Device Security Policy

The Mobile Device Policy covers the requirements specific to mobile devices with information storage or processing capabilities. This policy includes laptop standards, as well as requirements for PDAs, mobile phones, digital cameras and music players, and any other

removable device capable of transmitting, processing or storing information.

13. Vulnerability and Threat Management Policy

The Vulnerability and Threat Management Policy provides the requirements for patch management, vulnerability scanning, penetration testing, threat management (modeling and monitoring) and the appropriate ties to the Risk Management Policy.

14. Monitoring and Audit Policy

The Monitoring and Audit Policy covers the details regarding which types of computer events to record, how to maintain the logs, and the roles and responsibilities for how to review, monitor, and respond to log information. This policy also includes the requirements for backup, archival, reporting, forensics use, and retention of audit logs.

15. Project and System Development and Maintenance Policy

The System Development and Maintenance Policy covers the minimum security requirements for all software, application, and system development performed by or on behalf of Neustar and the minimum security requirements for maintaining information systems.