Internet Corporation for Assigned Names and Numbers ("ICANN")
12025 Waterfront Drive, Suite 300
Los Angeles, California 90094

Attention: New gTLD Program Staff

RE: Application for .Brand TLD Designation

VeriSign, Inc. ("Registry Operator"), in connection with the execution of the Registry Agreement for the .verisign TLD (the "Registry Agreement"), hereby applies for the .verisign TLD to be qualified by ICANN as a .Brand TLD.

Registry Operator confirms and represents to ICANN that the TLD meets each of the criteria for the TLD to be qualified as a .Brand TLD, as described in the .Brand TLD Application Process and Specification 13 attached thereto, and that all supplemental material accompanying this application is accurate and not misleading in any respect. Registry Operator also represents that the trademark registration attached hereto as Exhibit A, the registration policies attached hereto as Exhibit B, and the SMD file ID number attached hereto as Exhibit C are complete and accurate copies of the official trademark registration, Registry Operator's registration policies for the TLD, and the SMD file ID for the TLD for which this application is submitted, respectively.

Registry Operator agrees that if Registry Operator makes any changes to its registration policies for the TLD (whether before or after this application has been approved) that may disqualify the TLD as a .Brand TLD, it will promptly provide ICANN with a complete and accurate copy of the revised registration policies. In addition, if Registry Operator fails to maintain the trademark registration underlying its .Brand TLD application, it shall promptly notify ICANN of such failure. Registry Operator also agrees to maintain the criteria required to qualify as a .Brand TLD and to immediately notify ICANN of any changes in circumstances that could alter the statements made, and supporting materials provided with, this application.

Registry Operator acknowledges and agrees that this letter is binding on Registry Operator and, if any of the foregoing representations and agreements becomes untrue or not complied with, it shall be deemed a breach of the Registry Agreement by Registry Operator, and ICANN may assert its rights under the Registry Agreement, including by determining that the TLD no longer qualifies as a .Brand TLD pursuant to the terms of Specification 13.

Questions about this request should be directed to [redacted]

Submitted by: [redacted]
Position: SVP
Dated: August 28, 2014
Email: [redacted]

Exhibit A

Trademark Registration

Trademark RN 2758215: US Patent and Trademark Office; Registered September 2, 2003

Int. Cls.: 9, 16, 35, 36, 38, 40, 41 and 42

Prior U.S. Cls.: 2, 5, 21, 22, 23, 26, 29, 36, 37, 38, 50, 100, 101, 102, 103, 104, 106 and 107

Reg. No. 2,758,215

United States Patent and Trademark Office **Registered Sep. 2, 2003**

TRADEMARK
SERVICE MARK
PRINCIPAL REGISTER

VERISIGN

VERISIGN, INC. (DELAWARE CORPORATION)
21355 RIDGETOP CIRCLE
MAIL STOP LS3-3-4
DULLES, VA 20166

FOR: COMPUTER SOFTWARE IN THE FIELD OF CRYPTOGRAPHIC NETWORK SECURITY AND DATA SECURITY FUNCTIONS; COMPUTER SOFTWARE FOR INTEGRATION OF INFORMATION LOGIC AND DATA BETWEEN COMPUTER NETWORKS; COMPUTER SOFTWARE FOR AUTOMATING A PROCESS FOR AUTHENTICATION OF IDENTITY USING EXISTING DATABASES IN CONNECTION WITH THE ISSUANCE AND MANAGEMENT OF DIGITAL CERTIFICATES USED FOR AUTHENTICATION OR ENCRYPTION OF DIGITAL COMMUNICATIONS, OR AUTHENTICATION OF A DIGITAL SIGNATURE IN AN ELECTRONIC TRANSACTION OR COMMUNICATION, OVER THE INTERNET AND OTHER COMPUTER NETWORKS; COMPUTER SOFTWARE, NAMELY ENCRYPTION SOFTWARE TO ENABLE SECURE TRANSMISSION OF DIGITAL INFORMATION, NAMELY, CONFIDENTIAL, FINANCIAL AND CREDIT CARD INFORMATION OVER THE INTERNET AS WELL AS OVER OTHER MODES OF COMMUNICATION BETWEEN COMPUTING DEVICES; COMPUTER SOFTWARE TO INTEGRATE MANAGED SECURITY SERVICES, NAMELY PUBLIC KEY INFRASTRUCTURE (PKI) SERVICES, DIGITAL CERTIFICATE ISSUANCE, VERIFICATION, AND MANAGEMENT, AND ENTERPRISE SOFTWARE INTEGRATION, WITH EXISTING COMMUNICATIONS NETWORKS, SOFTWARE, AND SERVICES, DOWNLOADABLE ELECTRONIC PUBLICATIONS IN THE NATURE OF A NEWSLETTER IN THE FIELD OF INFORMATION TECHNOLOGY, IN CLASS 9 (U.S. CLS. 21, 23, 26, 36 AND 38).

FIRST USE 4-0-1995; IN COMMERCE 4-0-1995.

FOR: PRINTED MATTER, NAMELY, NEWSLETTERS, INSTRUCTIONAL MATERIALS AND TEACHING MATERIALS IN THE FIELD OF INFORMATION TECHNOLOGY, IN CLASS 16 (U.S. CLS. 2, 5, 22, 23, 29, 37, 38 AND 50).

FIRST USE 6-9-2000; IN COMMERCE 6-9-2000.

FOR: COMMERCIAL INFORMATION AND DIRECTORY SERVICES; PROVIDING COMMERCIAL INFORMATION AND ON-LINE DIRECTORY INFORMATION SERVICES FOR LOCATING INTERNET AND OTHER COMPUTER NETWORK ADDRESSES AND DEMOGRAPHIC INFORMATION FOR ENTITIES, AND PROVIDING A DIRECTORY OF ORGANIZATIONS, INDIVIDUALS, ADDRESSES, AND RESOURCES ACCESSIBLE THROUGH THE USE OF THE INTERNET AND OTHER COMPUTER NETWORKS; BUSINESS MANAGEMENT SERVICES, NAMELY, PROVIDING OUTSOURCE MANAGEMENT SERVICES TO OTHERS IN THE FIELD OF DIGITAL CERTIFICATE AUTHENTICATION; AUCTIONEERING SERVICES FOR DOMAIN NAMES ON THE INTERNET AND OTHER COMPUTER NETWORKS; ON-LINE TRADING SERVICES IN WHICH SELLER POSTS PRODUCTS TO BE AUCTIONED AND BIDDING IS DONE VIA THE INTERNET AND OTHER COMPUTER NETWORKS; ON-LINE RETAIL SERVICES FEATURING A VARIETY OF GENERAL MERCHANDISE; REFERRAL SERVICES IN THE FIELD OF VALUATION, FINANCING, PURCHASE AND SALE OF WEB-BASED BUSINESSES; AND COMPUTER NETWORK ADDRESS MANAGEMENT SERVICES, NAMELY, PROVIDING SERVICES ENABLING ENTITIES TO ACCESS, ADD, MODIFY OR DELETE INFORMATION RELATING TO THEIR COMPUTER NETWORK ADDRESSES, IN CLASS 35 (U.S. CLS. 100, 101 AND 102).

FIRST USE 4-0-1995; IN COMMERCE 4-0-1995.

FOR: INSURANCE SERVICES, NAMELY, INSURANCE BROKERAGE SERVICES AND ADMINISTRATION AND PROCESSING OF CLAIMS, FOR INSURANCE COVERING COMPUTER AUTHENTICATION, ENCRYPTION AND CERTIFICATION SERVICES FOR ELECTRONIC TRANSACTIONS AND COMMUNICATIONS THAT TAKE PLACE OVER THE INTERNET AND OTHER COMPUTER NETWORKS; PROVIDING EXTENDED WARRANTIES FOR AUTHENTICATION, ENCRYPTION AND CERTIFICATION SERVICES USED TO PROVIDE SECURITY IN ELECTRONIC TRANSACTIONS AND COMMUNICATIONS THAT TAKE PLACE OVER THE INTERNET AND OTHER COMPUTER NETWORKS; ADMINISTRATION AND PROCESSING OF CLAIMS UNDER EXTENDED WARRANTIES OF AUTHENTICATION, ENCRYPTION AND CERTIFICATION SERVICES USED TO PROVIDE SECURITY IN ELECTRONIC TRANSACTIONS AND COMMUNICATIONS THAT TAKE PLACE OVER THE INTERNET AND OTHER COMPUTER NETWORKS; FINANCIAL SERVICES, NAMELY PROVIDING FINANCIAL TRANSACTION PROCESSING SERVICES BY ELECTRONIC MEANS VIA THE INTERNET AND OTHER COMPUTER NETWORKS IN THE FIELD OF ELECTRONIC FUND TRANSFER AND PAYMENT PROCESSING SERVICES; BROKERAGE AND ESCROW SERVICES RELATING TO THE PURCHASE AND SALE OF DOMAIN NAMES, WEBSITES AND INTERNET BASED BUSINESSES; DOMAIN NAME VALUATION SERVICES; FINANCIAL MANAGEMENT SERVICES FOR ELECTRONIC DELIVERY, PROCESSING AND TRANSFER OF FUNDS, PAYMENTS, FINANCIAL TRANSACTIONS AND FINANCIAL INFORMATION VIA THE INTERNET AND OTHER COMPUTER NETWORKS , IN CLASS 36 (U.S. CLS. 100, 101 AND 102).

FIRST USE 2-29-2000; IN COMMERCE 2-29-2000.

FOR: PERSONALIZED ELECTRONIC MAIL SERVICES; E-MAIL FORWARDING AND WEB SITE FORWARDING, IN CLASS 38 (U.S. CLS. 100, 101 AND 104).

FIRST USE 12-0-2000; IN COMMERCE 12-0-2000.

FOR: DESIGN AND PRODUCTION OF CUSTOMIZED GOODS, NAMELY CUSTOMIZED PRINTING, SILK SCREEN PRINTING AND EMBROIDERY OF COMPANY NAMES AND LOGOS FOR PROMOTIONAL ADVERTISING PURPOSES ON THE GOODS OF OTHERS, IN CLASS 40 (U.S. CLS. 100, 103 AND 106).

FIRST USE 6-9-2000; IN COMMERCE 6-9-2000.

FOR: EDUCATIONAL SERVICES, NAMELY, PROVIDING INSTRUCTION AND DEMONSTRATIONS IN THE FIELDS OF USE AND MANAGEMENT OF COMPUTER NETWORKS, CORPORATE LOCAL AREA NETWORKS, THE INTERNET, COMPUTER NETWORK ADDRESSES, AND INTERNET DOMAIN NAME ISSUES; PROVIDING NEWS IN THE NATURE OF CURRENT EVENT REPORTING IN THE FIELD OF DOMAIN NAME DISPUTES; PROVIDING A NON-DOWNLOADABLE ON-LINE NEWSLETTER IN THE FIELD OF INFORMATION TECHNOLOGY , IN CLASS 41 (U.S. CLS. 100, 101 AND 107).

FIRST USE 6-9-2000; IN COMMERCE 6-9-2000.

FOR: PROVIDING AUTHENTICATION OF IDENTITY; ISSUANCE AND MANAGEMENT OF DIGITAL CERTIFICATES FOR AUTHENTICATION OR ENCRYPTION OF A DIGITAL COMMUNICATION, OR AUTHENTICATION OF A DIGITAL SIGNATURE IN AN ELECTRONIC TRANSACTION OR COMMUNICATION, OVER THE INTERNET AND OTHER COMPUTER NETWORK AND PROVIDING TECHNICAL AND CUSTOMER SUPPORT IN CONNECTION THEREWITH; DEVELOPMENT, DESIGN, IMPLEMENTATION, TESTING, ANALYSIS, AND CONSULTING SERVICES IN THE FIELD OF SECURITY, ACCESS, AUTHORIZATION, AUTHENTICATION ENCRYPTION, AND IDENTIFICATION SYSTEMS FOR COMPUTERS, COMPUTER HARDWARE AND COMPUTER NETWORKS; DEVELOPMENT, INTEGRATION AND OPERATION OF COMPUTER SYSTEMS TO SUPPORT ISSUANCE AND MANAGEMENT OF DIGITAL CERTIFICATES; CREATION AND IMPLEMENTATION OF PROCEDURES AND PRACTICES FOR ISSUANCE AND MANAGEMENT OF DIGITAL CERTIFICATES; COMPUTER RELATED SERVICES, NAMELY, MANAGED COMPUTER NETWORK AND INTERNET SECURITY SERVICES, NAMELY, PUBLIC KEY INFRASTRUCTURE ("PKI") VERIFICATION, AUTHENTICATION, DISTRIBUTION AND MANAGEMENT, DIGITAL CERTIFICATE ISSUANCE, VERIFICATION AND MANAGEMENT, AND ENTERPRISE SOFTWARE INTEGRATION; COMPUTER SERVICES, NAMELY, PROVIDING ONLINE INFORMATION IN THE FIELD OF DOMAIN NAME DISPUTES; COMPUTER SERVICES, NAMELY, ENABLING USERS OF THE INTERNET TO DELIVER INFORMATION ABOUT THEMSELVES AND, IF APPLICABLE, THEIR BUSINESSES, PRODUCTS OR SERVICES TO, AND TO REGISTER THEIR UNIVERSAL RESOURCE LOCATORS WITH ON-LINE CATALOGUES, DIRECTORIES, SEARCH ENGINES AND WEB SITES, VIA THE INTERNET AND OTHER COMPUTER NETWORKS; REGISTRATION AND TRACKING OF DOMAIN NAMES FOR IDENTIFICATION OF USERS ON A GLOBAL COMPUTER NETWORK AND OTHER COMPUTER NETWORKS; PROVIDING INFORMATION IN THE FIELD OF SERVICES RELATING TO THE OWNERSHIP RIGHTS OF DOMAIN NAMES; DOMAIN NAME MANAGEMENT SERVICES, NAMELY, DOMAIN NAME SYSTEM ("DNS") MANAGEMENT AND MAINTENANCE, DOMAIN NAME DIRECTORY MANAGEMENT AND MAINTENANCE, DOMAIN NAME SYSTEM ("DNS") INFRASTRUCTURE SERVICES, DOMAIN NAME AND DOMAIN NAME SYSTEM ("DNS") INFORMATION PROPAGATION, AND RESOLUTION OF DOMAIN NAME SYSTEM ("DNS") REQUESTS DATA CONVERSION OF COMPUTER PROGRAMS DATA OR INFORMATION, NAMELY, NETWORK, COMPUTER, DATABASE AND DIRECTORY SERVICES THAT CONVERT AN EXISTING TELEPHONE

NUMBER OR ASSIGNED NUMBER SEQUENCE INTO AN INTERNET PROTOCOL ("IP") ADDRESS OR UNIFORM RESOURCE LOCATOR ("URL") FOR THE PURPOSE OF ENABLING ACCESS, SELECTION AND DISPLAY OF ONLINE CONTENT VIA A WIRELESS NETWORK; COMPUTER SERVICES, NAMELY, MONITORING DOMAIN NAMES FOR CHANGE IN STATUS AND AFTER-MARKET AVAILABILITY; COMPUTER SERVICES, NAMELY, WEBSITE DESIGNING, HOSTING AND MAINTAINING SITES FOR OTHERS; PROVIDING TEMPLATES FOR DESIGN OF WEBSITES VIA ELECTRONIC COMMUNICATION NETWORKS; ON-LINE TECHNICAL SUPPORT SERVICES, NAMELY, TROUBLESHOOTING OF COMPUTER HARDWARE AND SOFTWARE PROBLEMS; COMPUTER SERVICES, NAMELY, PROVIDING SEARCH ENGINES FOR OBTAINING DATA ON A GLOBAL COMPUTER NETWORK; COMPUTER CONSULTATION REGARDING COMPUTER NETWORKS AND INTERNAL COMPUTER NETWORKS, SECURITY SERVICES FOR COMPUTER NETWORKS AND INTERNAL COMPUTER NETWORKS, NAMELY, DESIGNING FIRE WALLS FOR OTHERS; COMPUTER SOFTWARE CONSULTATION SERVICES FOR THE DEVELOPMENT OF SOFTWARE APPLICATIONS; DESIGNING AND PROGRAMMING COMPUTER CONTROLLED COMMUNICATIONS SYSTEMS, IN CLASS 42 (U.S. CLS. 100 AND 101).

FIRST USE 4-0-1995; IN COMMERCE 4-0-1995.

OWNER OF U.S. REG. NO. 2,302,350.

SER. NO. 76-389,499, FILED 3-28-2002.

BRENDAN MCCAULEY, EXAMINING ATTORNEY

Exhibit B

TLD Registration Policies

.VERISIGN Registration Policies

Per the .verisign application (1-1145-77950), VeriSign, Inc. will implement the following Registration Policies:

1. Eligibility

Registrations of domain names for the .verisign gTLD may only be performed by an authorized registrant acting on behalf of VeriSign, Inc. All domain name registrations in the gTLD will be registered to and maintained by VeriSign, Inc. for our own exclusive use. VeriSign, Inc. does not currently plan to sell, distribute, or transfer control or use of any registrations in the gTLD to any third party that is not an affiliate. Verisign intends to implement registration policies that: (i) require Verisign to approve any and all registrations; (ii) require all registrations to be in the name of Verisign and/or our affiliates; and (iii) require that control of such registrations and their use remain with Verisign and/or our affiliates and partners.

2. Privacy

As the sole registrant for the .verisign gTLD, we will publish all required registrant information in our Whois system, which will not contain private or confidential information. We will also publish Verisign contact and customer support contact information on our .verisign website. To the extent .verisign allows registrations by individuals, Verisign will protect such confidential information of such registrants in substantially the same manner as it protects the confidential information of registrants in .name.

Website Visitors. The .verisign gTLD serves as the destination point for our channel and alliance partners. We use .verisign second-level domain names as secure, personalized entry points that partners can access. Each custom entry point provides customized co-marketing assets, information, and other resources relevant to the partner's business and / or its customers' needs. Verisign controls all content.

We ask customers for consent to collect personal information for the following purposes:

- Email Request for Information or Registrations for Guides or Seminars. Links throughout our website enable customers to contact us via email to ask questions, request information and materials, register for guides or seminars, or provide comments and suggestions. We also offer customers the opportunity to have one of our representatives contact them personally to provide additional information about our products or services. To help us satisfy the customer's request, we may request additional personal information, such as the customer's name and telephone number.
- Enrollment. If a customer enrolls for one of our products or services, we request certain information. Depending on the type of product or service, we may ask the customer to provide his/her name, address, telephone number, email address, credit card number, bank account information, IP address, and/or Social Security number.

We take reasonable steps to protect this personal data from loss, misuse, unauthorized disclosure, alteration, or destruction. We do not use or authorize the use of personal data in a way that is incompatible with the verification and confirmation of the customer authorized use of the data. In addition, at a minimum, we scan the website daily to ensure customers are not exposed to malicious code.

2.1 Policies for Handling Complaints Regarding Abuse

Medium for External Complaints. External users of the system who have an abuse complaint (i.e., a researcher complaining of botnet activity or a user complaining of malware infection) can call Verisign Customer Service. Verisign's Customer Service includes the 24/7 onsite Customer Service Center (CSC) staff and on-call support from Tier 3 teams (e.g., registry operations staff, engineers, and developers) during non-business hours. Our primary concern is to resolve issues quickly and as such, we maintain a formal escalation process to ensure that all issues are addressed promptly by the "right" person/teams.

The CSC staff accepts every external complaint of malicious abuse of the .verisign gTLD's domain names, websites, or Domain Name System (DNS).

Our key performance metrics support timely response to customers' complaints of abuse. Our CSC answers 90 percent of phone calls within 20 seconds. Team leads actively manage all access channels to ensure appropriate responsiveness via each access channel.

Medium for Internal Complaints. Because the .verisign gTLD is used exclusively by Verisign, it is not available to the general public. Only Verisign and its affiliates are permitted to be registrants of .verisign domain names. Any security incidents or breaches noted by the registrant are reported to Verisign's formal Incident Response Team.

The Incident Response Team (IRT) is supported by a Corporate Incident Management Team (CIMT) and business-unit Business Continuity teams. These teams respond to and manage any incident or disaster that impacts Verisign employees, operations, environments, or facilities. To provide a secure and sound backup operational environment, our IT disaster recovery site has implemented the physical security protections and operational controls required by Verisign's overall Physical Security Program and Verisign's overall Information Security Program. In the event of an incident or disaster that requires temporary or permanent cessation of operations from Verisign's primary facility, the Verisign IRT and CIMT initiate Verisign's business continuity and IT disaster recovery process.

3. Abuse Policies

Because the .verisign gTLD is used solely by Verisign and not as a gTLD for others to utilize, the potential for domain name abuse is greatly reduced.

Potential abuse is largely limited to the following areas:

Phishing. Verisign defines phishing as the use of fraudulent web pages that are designed to trick recipients into divulging sensitive data such as user names or passwords. The .verisign gTLD will increase Internet users' trust by allowing them to more easily identify the landing pages of our products and services as authentically Verisign's and not those of a third party that may be spoofing the site or operating a phishing scam. The .verisign gTLD provides credibility that the inventions and data we share through this gTLD come directly from Verisign.

Willful Distribution of Malware: Verisign defines the willful distribution of malware as the dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, keylogging, and trojan horses. Verisign, as the trusted provider of registry services for the world's largest TLDs (e.g., .com and .net), is uniquely positioned to detect malware attacks on our sites. We have developed proprietary code to help identify malware in the zones we manage, which in turn enables us to identify malicious code hidden in our own domain names. Our malware scanning service helps prevent our websites from infecting other websites by scanning web pages for embedded malicious content that could potentially infect visitors' websites. Our malware scanning technology uses a combination of in-depth malware behavioral analysis, anti-virus results, detailed malware patterns, and network analysis to discover known exploits for the particular scanned zone.

4. Name Selection

Second-Level Domain Name Registration. We use the .verisign gTLD in the promotion and communication of the new Verisign brand and in product marketing efforts. We may use second-level domain names to create secure and personalized access to content, resources, and information for these brand and product marketing efforts. The .verisign second- level domains are registered exclusively by VeriSign, Inc. ("Verisign") and are not available to the general public. Only authorized employees of Verisign are permitted to register .verisign domain names on behalf of Verisign or an eligible affiliate. Second-level domains are signed using DNSSEC, secured with Verisign's Registry Lock service, scanned for malware using MalDetector, and monitored using our suite of security tools.

The .verisign gTLD will allow us to better differentiate our unique products and services by identifying the landing pages of such products and services as authentically Verisign's. This identification will allow customers to feel secure that the information they are receiving is coming from Verisign and its authorized affiliates and not a third party that may be spoofing the site or operating a phishing scam. The .verisign gTLD will also provide credibility that the inventions and data we share through this gTLD come directly from Verisign.

Authentication of Registrant Information. Registrations of .verisign domain names require the registrant to enter a valid Verisign employee ID to begin the registration process. Registrant data is cross referenced against the Verisign employee directory to validate the accuracy of the contact information. In addition, as part of the Registry-Registrar Agreement the registrar uses two-factor authentication to validate that the registrant data is accurate.

5. Monitoring of Registration Data for Accuracy and Completeness

Verisign has the capability to regularly validate registration data against our employee records to confirm that the registration data remains accurate. We investigate and correct any discrepancies within a reasonable period of time. Further, at least once per year and in accordance with ICANN's consensus policy relating to Whois accuracy, we ask each registrant to review and confirm the validity of the Whois data for domain names for which the contact is named.

Verisign has established policies and procedures to encourage registrar compliance with ICANN's Whois accuracy requirements. We incorporate the following services into our full-service registry operations.

Registrar self-certification. The self-certification program consists, in part, of evaluations applied equally to all operational ICANN accredited registrars and conducted from time to time throughout the year. Process steps are as follows:

- Verisign sends an email notification to the ICANN primary registrar contact, requesting that the contact go to a designated URL, log in with his/her Web ID and password, and complete and submit the online form. The contact must submit the form within 15 business days of receipt of the notification.
- When the form is submitted, we send the registrar an automated email confirming that the form was successfully submitted.
- We review the submitted form to ensure the certifications are compliant.
- We send the registrar an email notification if the registrar is found to be compliant in all areas.
- If a review of the response indicates that the registrar is out of compliance or if we have follow-up questions, the registrar has 10 days to respond to the inquiry.
- If the registrar does not respond within 15 business days of receiving the original notification, or if it does not respond to the request for additional information, we send the registrar a Breach Notice and give the registrar 30 days to cure the breach.
- If the registrar does not cure the breach, we terminate the Registry-Registrar Agreement (RRA).

Whois data reminder process. Verisign regularly reminds registrars of their obligation to comply with ICANN's Whois Data Reminder Policy, which was adopted by ICANN as a consensus policy on 27 March 2003 (http://www.icann.org/en/registrars/wdrp.htm). We send a notice to all registrars once a year reminding them of their obligation to be diligent in validating the Whois information provided during the registration process, to investigate claims of fraudulent Whois information, and to cancel domain name registrations for which Whois information is determined to be invalid.

6. Acceptable Use Policies

The .verisign gTLD will be used by Verisign alone and not as a gTLD for others to utilize. For this reason, there will be no application process for using the .verisign gTLD, apart from an internal process for running our digital marketing and web presence activities.

7. Rights Protection Mechanisms

In addition to the Sunrise and Trademark Claims services, Verisign implements and adheres to RPMs post-launch as mandated by ICANN, and confirms that registrars accredited for the .verisign gTLD are in compliance with these mechanisms. Certain aspects of these post-launch RPMs may be administered on behalf of Verisign by Verisign-approved registrars.

These post-launch RPMs include the established Uniform Domain-Name Dispute-Resolution Policy (UDRP), as well as the Uniform Rapid Suspension System (URS) and Trademark Post-Delegation Dispute Resolution Procedure (PDDRP). Where applicable, we will implement all determinations and decisions issued under the corresponding RPM.

After a domain name is registered, trademark holders can object to the registration through the UDRP or URS. Objections to the operation of the gTLD can be made through the PDDRP.

The following descriptions provide implementation details of each post-launch RPM for the .verisign gTLD:

- UDRP: The UDRP provides a mechanism for complainants to object to domain name registrations. The complainant files its objection with a UDRP provider and the domain name registrant has an opportunity to respond. The UDRP provider makes a decision based on the papers filed. If the complainant is successful, ownership of the domain name registration is transferred to the complainant. If the complainant is not successful, ownership of the domain name remains with the domain name registrant. Verisign and entities operating on our behalf adhere to all decisions rendered by UDRP providers.

- URS: Verisign also provides for a Uniform Rapid Suspension (URS) system as specified in the Applicant Guidebook. Similar to the UDRP, a complainant files its complaint with a URS provider. The URS provider conducts an administrative review for compliance with the filing requirements. If the complaint passes administrative review, the URS provider sends Verisign, the registry operator for .verisign, a Notice of Complaint. Within 24 hours of receipt of the Notice of Complaint, Verisign places the subject domain name on "lock," which restricts all changes to the registration data but allows the name to continue to resolve. After the domain name is placed on lock, the URS provider notifies the registrant of the complaint. The registrant is then given an opportunity to respond. The URS provider must then conduct a review of the complaint and response based on the rules outlined in the Uniform Rapid Suspension System Draft Procedures in the Applicant Guidebook. If the complainant is successful, the registry operator is informed and the domain name is suspended for the balance of the registration period; the domain name will not resolve to the original website, but to an informational web page provided by the URS provider. If the complainant is not successful, the lock is removed and full control of the domain name registration is returned to the domain name registrant. Similar to the existing UDRP, Verisign and entities operating on our behalf will adhere to the decisions rendered by the URS providers.

- PDDRP: Verisign also implements a PDDRP for the .verisign gTLD as provided in the Applicant Guidebook. The PDDRP provides a mechanism for a complainant to object to the registry operator's manner of operation or use of the gTLD. The complainant files its objection with a PDDRP provider, who performs a threshold review. The registry operator has the opportunity to respond and the provider issues its determination based on the papers filed, although there may be opportunity for further discovery and a hearing. Verisign implements the PDDRP process as specified in the Applicant Guidebook.

Additional Measures Specific to Rights Protection. Verisign provides additional measures against potentially abusive registrations. These measures help mitigate phishing, pharming, and other Internet security threats. The measures exceed the minimum requirements for RPMs defined by Specification 7 of the Registry Agreement and are available at the time of registration. These measures include:

- Rapid Takedown or Suspension Based on Court Orders: We comply with orders from courts of competent jurisdiction that direct Verisign to take any action on a domain name that is within our technical capabilities as a TLD registry. Courts may issue such orders when abusive content, such as child pornography, counterfeit goods, or illegal pharmaceuticals, is found to be associated with a subject domain name.

- Anti-Abuse Process: We implement an anti-abuse process that is executed based on the type of domain name takedown requested. The anti-abuse process is for malicious exploitation of the DNS infrastructure, such as phishing, botnets, and malware.

- Authentication Procedures: We use two-factor authentication to augment security protocols for telephone, email, and chat communications.

- Registry Lock: This Verisign service allows registrants to lock a domain name at the registry level to protect against both unintended and malicious changes, deletions, and transfers. Only Verisign can release the lock; thus all other entities that normally are permitted to update Shared Registration System (SRS) records are prevented from doing so. This lock is released only after the registrar makes the request to unlock.

- Malware Code Identification: This safeguard reduces opportunities for abusive behaviors that use registered domain names in the gTLD. Registrants are often unknowing victims of malware exploits. We have developed proprietary code to help identify malware in the zones we manage, which in turn helps registrars by identifying malicious code hidden in their domain names.

- DNSSEC Signing Service: Domain Name System Security Extensions (DNSSEC) helps mitigate pharming attacks that use cache poisoning to redirect unsuspecting users to fraudulent websites or addresses. It uses public key cryptography to digitally sign DNS data when it comes into the system and then validate it at its destination. The .verisign gTLD is DNSSEC-enabled as part of our core registry services.

Exhibit C

Signed Mark Data File ID Number: [redacted]