CONSUMER SENTINEL NETWORK CONFIDENTIALITY AND DATA SECURITY AGREEMENT

This agreement is entered into between the Bureau of Consumer Protection ("Bureau") of the Federal Trade Commission ("FTC") and the _____ ("Applicant"), in conjunction with all other domestic and foreign agencies and other entities similarly agreeing. The purpose of this agreement is to facilitate the confidential exchange of consumer complaint information, including information about consumer fraud and deception perpetrated through the Internet, direct mail, telemarketing, or other media, under the conditions set forth below.

The Consumer Sentinel Network

1. The FTC, in conjunction with the National Association of Attorneys General, Canshare, and PhoneBusters, has developed the Consumer Sentinel--an automated database to store investigatory information provided by participating law enforcement agencies and other contributors about consumer fraud and deception. Pursuant to the Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. §1028, the FTC also has developed the Identity Theft Data Clearinghouse--an automated database to store investigatory information provided by consumers, participating law enforcement agencies, and other contributors about identity theft. The FTC makes information contained in the Consumer Sentinel and the Identity Theft Data Clearinghouse available through the Consumer Sentinel Network. The information contained in both databases is known collectively as "Consumer Sentinel Network" information. This information exchange program is consistent with Section 6 (f) of the Federal Trade Commission Act, 15 U.S.C. § 46(f), Commission Rules 4.6, 4.10, and 4.11(c) and (d), 16 C.F.R. §§ 4.6, 4.10, and 4.11(c) and (d) (2010), and the Privacy Act of 1974, as amended, 5 U.S.C. § 552a. See also FTC Privacy Act system notices for consumer information (including identity theft) and National Do Not Call Registry records, as well as other potentially applicable systems at http://www.ftc.gov/foia/listofpaysystems.shtm, for routine uses of these records.

2. The information contained in the Consumer Sentinel Network does not include confidential commercial material, but is limited to information derived primarily from consumer complaints and other information gathered during identity theft, fraud, and other consumer protection investigations. This information may include, among other things, the names of companies and company representatives; the identity of the products or services involved; the status of ongoing law enforcement actions; and the names and telephone numbers of assigned staff.

Data Contribution from Participants

3. The signing entities and other data contributors may enter relevant information into one or both databases through the use of computer terminals located in their offices or by providing such information to other participants who will input such data into the system. Where necessary, the FTC subsequently loads this information into the automated databases, which are controlled by the FTC.

Access to Consumer Sentinel Network Information

4. Information in the Consumer Sentinel Network shall be made available as follows:

a. Information in the Consumer Sentinel database will be available only to the FTC and participating domestic and foreign law enforcement agencies that sign a Consumer Sentinel Network confidentiality and data security agreement. The form, substance and extent of disclosures to foreign law enforcement agencies shall be within the discretion of the FTC, subject to mutual agreement between the FTC and the foreign law enforcement agency.

b. Information in the Identity Theft Data Clearinghouse will be made available to the FTC and participating domestic and foreign law enforcement agencies that sign a Consumer Sentinel Network confidentiality and data security agreement. The form, substance and extent of disclosures to foreign law enforcement agencies shall be within the discretion of the FTC, subject to mutual agreement between the FTC and the foreign law enforcement agency. Limited information from the Identity Theft Data Clearinghouse also will be available to other participating domestic government agencies, consumer reporting agencies, and private entities that sign this agreement, to the extent consistent with the Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. §1028, and the Privacy Act, 5 U.S.C. 552a. The form and substance of disclosures to other participating domestic government agencies, consumer reporting agencies, and private entity participants is at the discretion of the FTC.

Confidentiality and Use of Consumer Sentinel Network Information

5. All parties participating in this information exchange system do so with the understanding that all Consumer Sentinel Network information, including all information available on the Consumer Sentinel Network's restricted website, will be kept confidential. In particular, the party signing this agreement agrees not to release such information to anyone other than its employees, consultants and contractors, or bona fide law enforcement agency personnel who are bound by this agreement and have a need to know such information. The FTC reserves the right to limit or revoke access to such information by any participating agency or other entity that breaches any of the terms of this agreement.

6. The party signing this agreement agrees to use information contained in the Consumer Sentinel Network in the manner indicated below (check only one designation):

a. _____ The party signing this agreement is a domestic or foreign law enforcement agency and agrees to use the Consumer Sentinel Network information to which it has access under paragraph 4 of this agreement only in connection with law enforcement purposes.

OR

b. _____ The party signing this agreement is a participating domestic government agency, consumer reporting agency, or private entity, and agrees to use the limited Identity Theft Data Clearinghouse information disclosed to it only to prevent or investigate frauds described in 18 U.S.C. § 1028 (a), subject to such additional conditions as designated by the FTC.

7. Except as authorized by law, the Bureau agrees that information contained in the Consumer Sentinel Network will not be released to anyone other than participating agencies and other entities as delineated in this agreement, and to employees of and consultants and contractors of such entities and of the FTC with a need to know such information. Should the FTC receive an official request from another federal law enforcement agency or from Congress[1] or should the FTC be directed to furnish information in the Consumer Sentinel Network to a nonparticipant by a court with jurisdiction to issue such an order, however, the FTC may, in its discretion, furnish that information subject to applicable statutory restrictions and in a manner consistent with the need to preserve the confidentiality of that information. In addition, the FTC will make aggregate statistics available to participants upon request and will continue to release trend data to the general public.

8. The signing party agrees that, should it receive a request for access to this material or should that information become subject to compulsory process, it will immediately notify the FTC contact person of these facts so that a timely decision can be made on whether to furnish the requested information and, if the information is to be furnished, how to furnish it in a manner that will preserve its confidentiality.

9. The FTC has appointed the Associate Director for Planning and Information, Bureau of Consumer Protection, to be its contact person for purposes of this

---

[1] It is the FTC's policy to provide information to Congress upon official request, although the Federal Trade Commission will request that the confidentiality of the information be maintained.

information exchange program with respect to domestic agencies and other entities. This official is responsible for ensuring the confidentiality of the information contained in the Consumer Sentinel Network and, in appropriate circumstances, for authorizing participants to make further disclosures of the material in response to requests for access or compulsory process. The Associate Director has also been delegated authority from the Commission to respond to requests for access from domestic law enforcement agencies to any FTC documentary materials relating to consumer fraud. Such requests will be handled under the procedures set forth in Commission Rule 4.11(c), 16 C.F.R. § 4.11(c), whereby the requesting party must submit a certification that the material will be used for law enforcement purposes and be kept confidential. The Commission has delegated to the Director, Office of International Affairs, the authority to execute Consumer Sentinel Network confidentiality agreements with any foreign law enforcement agency whose access has been authorized or is authorized in the future by the Commission or by the Commission's delegate. The Commission has also delegated to the Director, Office of International Affairs, authority to disclose certain nonpublic information to foreign law enforcement agencies. Such execution of confidentiality agreements with foreign law enforcement agencies and such disclosure to foreign law enforcement agencies shall be pursuant to 67 FR 45738 (2002) or other Federal Register notices or rules published by the Commission. The Director of the Bureau of Consumer Protection, subject to redelegation, may also respond to foreign access requests for certain information on consumer protection pursuant to the delegation authority set forth at 62 Fed. Reg. 15185 (1997).

Data Security and Minimum Safeguards

10. The Consumer Sentinel Network contains personally identifiable information about consumers including identity theft and fraud victims, as well as individuals who are identified by the complainants as subjects. Although we do not require them to do so, consumers sometimes provide highly sensitive information about bank accounts, credit cards, their medical history, and Social Security numbers in the comments field of complaints. It is critical that you keep this information secure. Even a consumer's name and phone number, in conjunction with other information, can be used by fraudsters and identity thieves. The FTC takes its responsibility as custodian of consumer data and trust very seriously, and expects members of the Consumer Sentinel Network to do the same. Therefore, those wishing to become members of the Consumer Sentinel Network must agree to maintain the data in a confidential and secure manner.

11. As a member of the Consumer Sentinel Network, and as a signatory to this agreement, the Applicant is responsible for ensuring the privacy and security of the information which it has agreed to keep confidential. The Applicant must maintain and/or implement the minimum safeguards contained in this agreement, in order to access the Consumer Sentinel Network, and to comply with the terms and

conditions contained in this agreement.

a. Extracts, Downloads, and Printouts – Applicant shall ensure that any information printed, downloaded or otherwise removed from the Consumer Sentinel Network (either in an electronic or in a printed format) is properly protected. Applicant must ensure that all such information is deleted and destroyed within 90 days unless its use is still required for law enforcement purposes. This includes Consumer Sentinel Network information that has been inserted in a spreadsheet or another database, or which has been printed or copied into any other form.

    i. For Consumer Sentinel Network information that has been saved in a paper format (e.g. printed documents), Applicant must ensure that the information is secured in a locked drawer or file cabinet.

    ii. For Consumer Sentinel Network information that has been saved in an electronic format, Applicant must use encryption compliant with the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules 140-2 (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf) such as PKWARE's SecureZIP or a WinZIP version 11.1. A list of products compliant with this standard is located at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm. In addition, if Consumer Sentinel Network information is stored on a portable computing device and/or media (e.g. laptop computer, CD/DVD, USB device, etc.), then that device and/or media must be properly secured and locked (e.g. lock portable computing devices and/or media in a drawer or file cabinet; properly secure laptops via locking security cables; etc.).

b. Proper Disposal – Applicant shall ensure the proper disposal of Consumer Sentinel Network information.

    i. For Consumer Sentinel Network information that has been saved in a paper format (e.g. printed documents), Applicant must ensure that such documents are burned, pulverized, or shredded in a manner that ensures that the information cannot practicably be read or reconstructed.

    ii. For Consumer Sentinel Network information that has been saved in an electronic format, Applicant must destroy or erase Consumer Sentinel Network information in a manner that ensures that the information cannot practicably be read or reconstructed. Proper erasure of electronic information must include the overwriting or

"wiping" of the information from the electronic media on which it is stored.

c. Computer Usage – Applicant shall allow access to Consumer Sentinel Network information and the Consumer Sentinel Network only from computers issued and maintained by Applicant's organization. When accessing the Consumer Sentinel Network, such computers shall be secured within Applicant's facilities (i.e. within Applicant's buildings). In addition, such computers shall at all times be protected from viruses, malware, and other exploits, by

    i. usage of up-to-date firewall, anti-virus, and anti-spyware programs, whose software and support files (e.g. virus signatures) are automatically kept up-to-date;

    ii. usage of up-to-date web browsers whose security settings are set at the highest level available for that browser; and

    iii. installation of up-to-date security patches for your operating systems and browsers.

d. UserIDs, Passwords, and Tokens – Applicant shall ensure that Consumer Sentinel Network log in user IDs, passwords, and tokens are properly secured.

    i. Applicant will ensure that user IDs, passwords, and tokens are not shared.

    ii. Applicant will ensure that computers/browsers will not be configured to "remember" user IDs and passwords.

    iii. Applicant shall ensure that open Consumer Sentinel Network sessions will not be left running on an unattended or an unlocked computer.

e. Need-to-Know – Applicant shall ensure that access to the Consumer Sentinel Network and to Consumer Sentinel Network information is limited to those individuals in Applicant's organization who need access to such information.

f. Data Breach Notification – Applicant shall respond to the loss of Consumer Sentinel Network information as set forth below.

    i. Applicant shall notify the FTC, both orally and by email, within

one hour of discovery/detection of the following:

1. when an unauthorized individual gains logical or physical access to Consumer Sentinel Network information or to the Consumer Sentinel Network;

2. when there is a suspected or confirmed breach of Consumer Sentinel Network information regardless of the manner in which it might have occurred; or

3. when a serious computer security incident occurs on a computer containing Consumer Sentinel Network information, or on a computer with access to the Consumer Sentinel Network, which may place at risk the Consumer Sentinel Network information or other users of the Consumer Sentinel Network.

Applicant's report shall identify: (i) the nature of the unauthorized use or disclosure; (ii) the Consumer Sentinel Network information used or disclosed; (iii) who made the unauthorized use or received the unauthorized disclosure; (iv) what Applicant has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and (v) what corrective action Applicant has taken or shall take to prevent future similar unauthorized use or disclosure. Applicant shall provide other information, including a written report, as reasonably requested by FTC.

ii. For incidents involving personally identifiable information, Applicant must consult with the FTC to determine whether notice and/or some form of mitigation (e.g. credit monitoring, data breach analysis, etc.) to affected individuals is required. In those circumstances where notice and/or mitigation is required, Applicant will be responsible for providing any such notice and/or mitigation, as well as for any reasonable costs associated with such notice and/or mitigation.

g. Training – Applicant shall ensure that individuals within Applicant's organization who access the Consumer Sentinel Network and/or Consumer Sentinel Network information understand their responsibilities under this agreement, and such additional terms of use as the FTC may from time to time adopt. In addition, all Consumer Sentinel Network users will be required to complete an on-line training module prior to gaining access to the system, and annually thereafter.

The individuals signing this agreement represent and warrant that they have all necessary rights, powers, and authority to enter into and perform this agreement. Further, the Applicant understands and acknowledges that any unauthorized access to, or unauthorized disclosure, transfer, alteration, destruction, or use of Consumer Sentinel Network information or the Consumer Sentinel Network shall be a violation of this agreement and may 1) be a basis for termination of Applicant's access to the Consumer Sentinel Network, and/or 2) represent a violation of the Privacy Act of 1974, the Computer Fraud and Abuse Act of 1986, or other applicable laws and authorities.

Consumer Sentinel Network Amendments

The following points below amend the Consumer Sentinel Network ("Sentinel") Confidentiality and Data Security Agreement ("Agreement"). All member agencies signed the Agreement upon registering for Sentinel. To retain or obtain access to Sentinel, all individual users must agree to the Agreement as well as the terms and conditions of the following Amendments.

The individual user acknowledges and agrees to the following terms and conditions without modification. Any concerns or questions can be directed to sentinel@ftc.gov.

Program Amendments

1. The Division of Planning and Information, Bureau of Consumer Protection is now the Division of Consumer Response and Operations ("DCRO"). The Associate Director of DCRO is now the point of contact referenced in Paragraph 9 of the Agreement.

2. The Identity Theft Data Clearinghouse is now the identity theft subset of complaint data within Sentinel. A member agency may choose to have optional additional access to that data as needed in addition to the default fraud and National Do Not Call Registry ("DNC") complaint data subsets. In effect, all member agencies are considered to have agreed to Paragraph 6(a) of the Agreement.

3. The appropriate purposes of using Sentinel data are as follows: 1) the investigation and/or prosecution of consumer fraud, identity theft, or DNC violations; 2) consumer and business education on these subjects; and 3) the creation of data analysis products.

4. DCRO may use any data received from a data contributor or a Sentinel user for the administration of the Sentinel program.

Technical Amendments

5. Mobile device usage of Sentinel must follow the same security standards as desktop and laptop devices detailed in Paragraph 5 and the basic Sentinel operational requirements. Mobile devices using a carrier-based IP rather than an agency approved IP will not have access to CSN PII data.

6. Paragraph 11(a.ii) is is modified to remove version specific FIPS 140-2 compliant encryption software (i.e., WinZip rather than WinZip version 11.1) and to use software that is up to date with patches and vendor support in accordance with CISA BOD 22-01. Similarly, paragraph 11(a.), 11(c) and 11(d) are modified to include general CISA BOD 22-01 compliance of user's operating system and applications. In addition, users' systems must follow federal government security guidelines including recent NIST SP800-53, OMB M-22-09, and NIST security measures for EO-critical software. This requires security features such as the use of multi-factor authentication for users' logins to their operating systems, FIP 140-2 compliant encryption of data at rest, endpoint security protection such as antivirus protection to secure operating systems, and security event logging and incident response as part of an agency operated continuous monitoring solution. Paragraphs 11(c) and 11(d) of the Agreement regulate appropriate access protocol, which presently include a Sentinel username, password, and two-factor authentication. The users must also meet the basic Sentinel operational requirements and access Sentinel from a designated Internet Protocol range through a Virtual Private Network as needed.

User Responsibilities

7. Paragraph 11(c) of the Agreement regulates where a Sentinel user can access data. This location is expanded beyond government offices to any routine location of teleworking or any designated temporary duty location, such as a litigation war room.

8. Sentinel data generally may only be shared with individual Sentinel member agencies. Law enforcement fusion centers and task forces are not exceptions. Users are permitted to share data in the prosecution of law enforcement actions (e.g. submitting data as evidence) or in achieving a law enforcement resolution through settlement negotiations or redress.

9. The requirements for Paragraph 8 of the Agreement are annulled. That is, the signing party is not required to routinely notify the FTC of access requests (e.g. compulsory process) unless the signing party needs guidance in that regard. The signing party is expected to abide by all the other confidentiality and data security restrictions in the Agreement and the Amendments.

10. Users will only download or print data when necessary to do so. Users are responsible for any downloaded or printed data and will destroy the data upon confirmation that it is no longer needed for law enforcement purposes. Media sanitization should follow federal standards including NIST 800-88 guidelines with

collection of evidence of this sanitization for audit purposes.

11. Violations of the Agreement or its Amendments may result in user and/or agency removal from the Consumer Sentinel Network.

The _____ agrees to the above Amendments.

Signature _____

Name:
Title:
Organization:

Address:

Phone Number:
Email Address:

Date _____

Signature _____

Maria Mayo
Associate Director
Division of Consumer Response and Operations
Federal Trade Commission
400 7th Street SW
Washington, DC 20024
(202) 326-3438
mmayo@ftc.gov

Date _____

FTC signature block for agreements with international organizations

Signature _____

Randolph W. Tritell
Director
Office of International Affairs
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
(202) 326-3051
rtritell@ftc.gov

Date _____