

CONSUMER SENTINEL NETWORK USER AGREEMENT

Access to the Consumer Sentinel Network and to Consumer Sentinel Network information is subject to the terms and conditions in the Consumer Sentinel Network Confidentiality and Data Security Agreement. By accessing the Consumer Sentinel Network you acknowledge that you have read the Consumer Sentinel Network Confidentiality and Security Agreement, and agree to be bound by its terms and conditions, which include the following:

1. Confidentiality - The Consumer Sentinel Network Confidentiality and Data Security Agreement requires you to treat information in the Consumer Sentinel Network in a confidential manner. Information in the Consumer Sentinel Network includes, but is not limited to, complaints, alerts, top violator and other reports, and reference materials. Information in the Consumer Sentinel Network must not be made public or shared with non-member agencies. This rule extends even to acknowledging the existence of complaints against a particular subject. Further, Consumer Sentinel Network information must be used only for law enforcement purposes. If you are compelled to disclose Consumer Sentinel Network information, please contact the FTC immediately so that we can determine if you can release the data and, if so, how to furnish it in a way to protect its confidentiality.

Importantly, 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 access the Consumer Sentinel Network must agree to maintain the data in a confidential and secure manner.

2. Access Only for Law Enforcement Purposes - The Consumer Sentinel Network Confidentiality and Data Security Agreement restricts access to the Consumer Sentinel Network to domestic or foreign law enforcement agencies that agree to use the Consumer Sentinel Network information only for law enforcement purposes. In addition, Consumer Sentinel Network information that is contained in the Identity Theft Data Clearinghouse may only be used to prevent or investigate frauds described in 18 U.S.C. § 1028 (a).
3. Data Security and Minimum Safeguards - The Consumer Sentinel Network Confidentiality and Data Security Agreement outlines the minimum safeguards and security controls you must use to ensure the privacy and security of Consumer Sentinel Network information.

- a. Extracts, Downloads, and Printouts – Users 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. Users 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), Users 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 – User 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), Users 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, Users 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 – Users shall access Consumer Sentinel Network information and the Consumer Sentinel Network only from computers issued and maintained by <insert organization name>. When accessing the Consumer Sentinel Network, such computers shall be secured within <insert organization name>'s facilities (i.e. within <insert organization name>'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 – Users shall ensure that Consumer Sentinel Network log in user IDs, passwords, and tokens are properly secured.
- i. Users will not share user IDs, passwords, and tokens.
 - ii. Users will not use computers/browsers configured to "remember" user IDs and passwords.
 - iii. Users shall not leave open Consumer Sentinel Network sessions running on an unattended or an unlocked computer.
- e. Need-to-Know – Users shall only access the Consumer Sentinel Network and Consumer Sentinel Network information for law enforcement purposes.
- f. Data Breach Notification – Users shall respond to the loss of Consumer Sentinel Network information as set forth below.
- i. Users 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.

Reports 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 <insert organization name> and Users have done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and

(v) what corrective action <insert organization name> and Users have taken or shall take to prevent future similar unauthorized use or disclosure. Users shall provide other information, including a written report, as reasonably requested by FTC.

ii. For incidents involving personally identifiable information, <insert organization name> and Users 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, <insert organization name> 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 – 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.

4. Unauthorized Access, Disclosure, or Use - Users understand and acknowledge that any unauthorized access to, or unauthorized disclosure, transfer, alteration, destruction, or use of Consumer Sentinel Network information or the Consumer Sentinel Network by the Users shall be a violation of this agreement and may 1) be a basis for termination of your organization'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.

Your continued use of the Consumer Sentinel Network will constitute your agreement to be bound by the terms and conditions set forth in the Consumer Sentinel Network Confidentiality and Security Agreement.