
# PRIVACY IMPACT ASSESSMENT (PIA) FOR:

# Sentinel Network Services (SNS)

**Previously CRSS**

**June 2008**
**(Updated January 2013)**

The Federal Trade Commission's (FTC) Bureau of Consumer Protection (BCP) protects consumers from a variety of fraudulent, deceptive, and unfair practices in the marketplace, including identity theft, telemarketing fraud, Internet fraud, and consumer credit issues. To further its consumer protection mission, the FTC brings civil and administrative law enforcement actions to enforce its laws and provides consumer and business education to enable the public to avoid common harms. The FTC works to ensure that consumers have accurate information for purchasing decisions, and confidence in the traditional and electronic marketplaces.

BCP's consumer protection-related activities include consumer complaint collection and analysis, individual company and industry-wide investigations, administrative and federal court litigation, rulemaking proceedings, consumer and business education, and the operation of consumer protection programs.

One focus of these activities is the enforcement of the Telemarketing Sales Rule (TSR) and do not call regulations (16 C.F.R. Part 310). BCP uses the National Do Not Call Registry® (DNC) to protect consumers from unwanted telemarketing sales calls and to make complaints about calls they receive; to assist telemarketers in complying with regulations; and assist law enforcement investigations of violations.

In addition, BCP uses the Consumer Response Center (CRC) to allow consumers to report instances of identity theft and other consumer protection complaints; to guide and educate consumers; and to assist law enforcement investigations of alleged violations. The CRC acts as both an information collection and dissemination point to assist in mission achievement.

BCP's consumer protection-related activities also include enforcement of the Controlling the Assault of Non-Solicited Pornography and Marketing Act (the CAN-SPAM Act of 2003, 15 U.S.C. § 7704), which establishes requirements for those who send commercial email, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask emailers to stop spamming them. To support BCP's investigations and consumer protection-related activities, BCP has created a "Spam Database" (SpamDB) where consumers can submit unsolicited commercial emails that they receive.

Consumer complaint information received by the FTC, including spam, is made available to thousands of civil and criminal law enforcement personnel in the United States and abroad through a secure Internet website called the Consumer Sentinel Network (CSN). CSN thus makes the complaint filing and collection process more efficient for both consumers and law enforcement; consumers file one complaint that can be accessed by numerous agencies, each of which may have jurisdiction and the ability to assist the consumer or prosecute the alleged violation. CSN is used to make available, analyze and extract data, and to provide a host of other investigatory tools to members.

BCP's DNC, CRC, SpamDB and CSN programs are collectively referred to as Sentinel Network Services (SNS). The FTC has contracted with Lockheed Martin Information Systems & Global

Services (LM IS&GS) to implement, maintain, and operate SNS. BCP has conducted this Privacy Impact Assessment on SNS as part of the Certification and Accreditation process for major information technology systems.

## 1.0 System Overview

SNS is a powerful consumer protection data source, much of which is available to the federal, state, local, and international law enforcement community. SNS data is also used to identify and track trends and potential problems affecting the marketplace. SNS contains data collected by the FTC as well as data collected by other entities and forwarded to the FTC. External contributors include a broad array of public and private domestic and foreign organizations.

SNS uses several applications or components to collect and share consumer data as described below. SNS related data is owned by BCP's Division of Planning and Information.

### 1.1 Consumer Response Center (CRC)

The Consumer Response Center gathers, processes and updates consumer information via call center services and Internet-based complaint forms. Users access a multi-channel bilingual (English and Spanish) contact center to file complaints, report instances of identity theft, receive and print an identity theft affidavit, and request or receive consumer education materials. Consumers may contact the CRC by using two toll-free telephone numbers, 1-877-FTC-HELP or 1-877-ID-THEFT. Toll-free services include:

- Interactive Voice Response (IVR)
- TTY (for hearing impaired persons)
- Live telephone conversations with customer service representatives

Consumers may also contact the CRC online by filing a complaint via the Complaint Assistant Wizard, which asks consumers to answer a series of questions organized in a few simple steps. Hyperlinks to the Complaint Assistant Wizard - https://www.ftccomplaintassistant.gov/ - are available through FTC.gov. The Complaint Assistant Wizard also has a portal called Military Sentinel, designed for members of the military filing a complaint. It asks all of the questions that the Complaint Assistant Wizard asks plus several additional questions that apply only to military members and are of assistance to military law enforcement.

Finally, consumers may contact the CRC through postal mail.

The CRC currently handles about 2 million consumer interactions per year - about 50% of these interactions are automated. Consumer complaint data received through the CRC is entered into CSN.

### 1.2 National Do Not Call Registry® (DNC)

DNC consists of four major functions: consumer registration, telemarketer access, law enforcement access, and consumer complaints. The consumer registration function allows consumers to register their telephone numbers and to verify whether their phone numbers are on the registry. Consumers carry out these activities through the secure Internet site at www.donotcall.gov or via nationwide toll-free telephone numbers (1-888-382-1222 or TTY 1-866-290-4236). Consumers may also delete their telephone numbers from the registry by using the toll-free system, if they are calling from the phone that is registered. Users of the consumer Internet site or toll-free telephone number may interact with DNC in English or Spanish. In addition, the telephone system supports hearing impaired persons through a toll-free number for teletypewriter (TTY) access.

Telemarketers may access DNC through the Internet site telemarketing.donotcall.gov. New telemarketers create a profile and receive an organization ID and password. They then subscribe to area codes their telemarketing campaign will call and, if required, pay for their subscription. Upon successful completion of that step, they download registered consumer telephone numbers within the selected area codes to ensure that they do not call those numbers. Telemarketers originally were required to download and scrub their lists every 90 days; in 2005, this was shortened to 31 days. Each time telemarketers access DNC, they must certify that their organization will comply with the DNC requirements. In addition, telemarketers may access an online helpdesk system to obtain assistance with technical questions and issues.

CSN law enforcement members in the United States, Canada, and Australia may access the DNC system to support investigations of violations of the Telemarketing Sales Rule. These Sentinel members can access information about the registration, verification, and deletion transactions for individual consumer telephone numbers. They may also gather information about telemarketer enrollment profiles, clients, subscriptions, and downloads.

Consumers may file complaints about alleged violations of the do not call rules through Donotcall.gov or by calling 1-888-382-1222. Like the registration function, consumers may access the complaint function either over the Internet or by telephone. Consumer complaint data received through DNC is made available to law enforcement on the CSN.

### 1.3 Spam Database (SpamDB)

The SpamDB provides the public with an email address (spam@uce.gov) to which they can forward email messages that they believe to be spam (also known as unsolicited commercial email). Participation is voluntary, and the Commission's website notifies consumers that the FTC maintains this information for use in law enforcement investigations.[1] Currently the system receives over 44 million submissions a year. Because spam email may contain viruses and other

[1] See http://www.ftc.gov/ftc/contact.shtm.

malware that can exploit security vulnerabilities, the SpamDB receives and processes all emails in an isolated cloud computing environment.[2] The SpamDB permits authorized CSN users to view a static image of the actual email to protect SNS and its users against any risks associated with spam email.

### 1.4 Consumer Sentinel® Network (CSN)

CSN includes the following series of interconnected websites:

- Consumer Sentinel® - general fraud, identity theft (IDT), DNC, consumer credit issues, and other complaints, accessed at www.consumersentinel.gov
- Consumer Planet Sentinel - cross-border e-commerce complaints, accessed at www.econsumer.ftccomplaintassistant.gov
- Consumer Sentinel/Military - fraud and identity theft complaints from military personnel, also accessed at www.consumersentinel.gov

Consumer Sentinel is the website through which local, state and federal law enforcement agencies in the United States, Canada, and Australia access complaints collected by the CRC directly from consumers or complaints collected by other entities and forwarded to the FTC. Included within Consumer Sentinel is the IDT Data Clearinghouse, which is the nation's repository of identity theft complaints. These complaints also are made available through CSN. As a further protection, identity theft complaints are only available to those law enforcement agencies who request access to that data.

The Consumer Planet Sentinel (CPS) website is also housed within CSN. CPS membership is open to government agencies in those countries that belong to the International Consumer Protection and Enforcement Network (ICPEN). CPS is part of econsumer.gov (www.econsumer.ftccomplaintassistant.gov), an international project focusing on cross-border e-commerce fraud. The econsumer.gov site offers cross-border consumer protection information and an additional separate online complaint form able to process consumer complaints in additional languages. All information on econsumer.gov, including the complaint form, is available in English, Spanish, French, German, Polish, Japanese, and Korean. Cross-border e-commerce complaints received from consumers through the econsumer.gov complaint form are entered into CSN. CPS users can access only those complaints received through econsumer.gov.

Military Sentinel is a joint initiative of the FTC and the Department of Defense (DOD) to identify and target consumer protection issues for service members, their families, and DOD civilians. Military Sentinel consists of a public Internet site and a restricted Internet site

---

[2]"Cloud computing is internet-based computing whereby shared resources, software, and information are provided to computers and other devices." CIO Council, "Privacy Recommendation for the Use of Cloud Computing by Federal Departments and Agencies" August 2010.

accessed through CSN. Military members wishing to file complaints may do so at //www.ftc.gov/sentinel/military/index.shtml. The Military Sentinel public site is a version of the Complaint Assistant Wizard that also provides a gateway to consumer education materials covering a wide range of consumer protection issues, including issues that are directed to members of the military. The complaint forms on the Military Sentinel public site allow consumers to identify their service branch, posting, and pay grade. Complaints entered into Military Sentinel go directly into, CSN, for access by authorized CSN users.

Authorized users access the CSN through a secure, password-protected Internet site which uses two-factor authentication. CSN users' access to the various subsets of data in the system is based on the organization to which they belong. For example, Canadian law enforcement has access to general fraud complaints but does not have access to complaints regarding credit reporting or various other complaints that are related specifically to a domestic law issue.

Authorized CSN users may search the complaint database using criteria which include company or suspect name, address, telephone number, consumer location, or type of scam or identity theft. As of August 2012, CSN served over 2,100 law enforcement agencies across the world that have signed appropriate confidentiality agreements restricting their use and disclosure of CSN data to law enforcement purposes.

CSN is an effective tool for immediate and secure access to consumer complaints about fraud, identity theft, Internet fraud, telemarketing, and consumer credit issues, among others. Authorized law enforcement users can utilize CSN to:

- Find complaints
- Store search results in 100 MB of online storage space
- Search within searches
- Gather related complaints using keywords in the search results
- Extract a limited number of complaints from the system for use in their investigations

## 2.0 Information Collected and Stored Within SNS

### 2.1 What information is collected, used, disseminated, or maintained by SNS?

The various SNS components collect and maintain personal information that consumers voluntarily submit when they contact the FTC to file a complaint or to request information. The CRC collects such information directly from consumers, or from their guardians or others acting on their behalf who may provide the information by using the CRC's Complaint Assistant Wizard found at ftc.gov, or by calling or writing to the CRC. Consumers may also submit similar information through the separate complaint forms found at econsumer.gov, or the

Military Sentinel complaint forms accessed at http://www.ftc.gov/sentinel/military/index.shtml. The personal information collected in these complaint forms may include:

- First and last name
- Street address, city, state, country and postal code
- Email address
- Date of birth only for IDT complaints or age range
- Contact telephone number(s)
- Social Security Number (SSN), only if applicable
- Relationship to suspect, only for identity theft complaints
- Account number, only for identity theft complaints
- Driver's license number, only for identity theft complaints
- Free-form description of the consumer's issue(s)

For two categories of complaints, identity theft-related complaints and complaints related to the accuracy of consumer credit reports, SNS includes a field for consumers to provide a SSN if they choose. Consumers submitting identity theft complaints are asked to provide their SSN in order to assist law enforcement with identity theft investigations. Consumers submitting complaints about the accuracy of consumer credit reports are asked to provide their SSNs to enable the consumer reporting agency (CRA) to accurately and efficiently match the consumer complaint to the CRA's files, pursuant to a statutory complaint sharing and resolution initiative (see section 3.3). SNS encrypts the SSN, and the number is not displayed when members search the system. SNS also collects and maintains the subject matter of consumers' complaints and information regarding the companies, entities, or individuals about which the consumer is complaining. If the complaint is reported by someone else on behalf of the consumer, then name, address, and contact information of the person reporting the complaint is also captured along with the affected consumer's information, and both are stored in CSN.

If a consumer submits their entire identity theft complaint by phone, but would like to print a copy of an affidavit of their complaint to provide to law enforcement, the counselor will provide them with a single-use password, and the consumer will receive an email with a secure custom link to a login page to access this form.

When a consumer files a police report related to identity theft, U.S. law enforcement with access to CSN can update the consumer's identity theft complaint that was submitted to the FTC. Law enforcement can update the consumer's complaint to include information about the department taking the police report, which includes the name of the department, report number, date of report, officer's name and the officer's telephone number. Law enforcement can also update the complaint to include new information provided by the consumer in the police report.

When a consumer complains about an individual, as opposed to a company or other entity, the CRC may collect the following personal information about the individual against whom the consumer is complaining:

- First and last name
- Middle name and suffix, only for identity theft complaints
- Street address, city, state, country and postal code
- Email address
- Telephone number(s)
- Date of birth, only for identity theft complaints
- SSN, only for identity theft complaints
- Individual's relationship to consumer, only for identity theft complaints
- Method individual used to obtain the complainant's personal information without authorization, only for identity theft complaints

In addition to the standard information collected on the CRC's other online complaint forms, the complaint forms on Military Sentinel allow consumers to identify their service branch, posting, and pay grade.

For system auditing purposes, SNS also collects and stores the following user responses, computer system and network related information along with the consumer complaints:

- Answers or responses provided by consumers to the questions presented by the online Complaint Assistant Wizard or the IVR while gathering their complaints
- Date and time when the consumer's complaint is submitted or updated
- Name of the domain and host from which the consumer gained access to the online complaint forms
- Internet address of the site from which the user linked directly to the online complaint forms
- Internet protocol (IP) address of the computer the consumer was using when submitting a complaint online
- User's Internet browser software information

SNS also includes consumer complaint data collected and forwarded to the FTC by external data contributors (see section 2.2). External data contributors include a broad array of public and private domestic and foreign law enforcement, consumer protection, and other organizations. The consumer complaint data collected from external data contributors includes the same types of data collected by the CRC.

DNC collects and maintains information that consumers voluntarily submit either via the Internet site or by calling the DNC's toll-free telephone numbers. For registrations, verifications, and deletions completed over the telephone, the only information provided by consumers is their telephone number. Consumers registering via the DNC website must also provide an email address, which is used as part of an online confirmation process that includes the delivery of an email message and online confirmation transaction. Importantly, the DNC registry uses a secure hash algorithm to maintain the security of consumer email address information. For consumers calling the DNC toll-free telephone numbers, access control is

limited by requiring them to call from the telephone that they wish to register, delete, or verify. The DNC only collects telephone numbers and the numbers are not associated with any other information, including email addresses.

For DNC complaints, consumers must provide the telephone number that the telemarketer called and when the telemarketer called. Optionally, consumers may also provide the name and/or the telephone number of the telemarketing company, their name and address, and additional comments. Consumers are cautioned not to provide personally identifiable information (PII) such as their SSNs. Consumers are also asked to answer the following three questions:

- Have you done business with this company in the last 18 months or contacted them in the last 3 months?
- Was this a pre-recorded message?
- Have you asked this company to stop calling you?

When telemarketers enroll and create their profiles, they must provide the following information: their organization name and address; Employer Identification Number (EIN) or SSN in the case of a sole proprietorship; organization contact person; and the contact person's telephone number and email address. If an entity is accessing the registry on behalf of a seller-client, the entity also will need to identify that client. Telemarketer payment information, including account numbers, is collected and handled by Pay.Gov[3], the federal government payment processor operated by the US Department of the Treasury, and is not shared with the FTC.

Telemarketers who submit requests to DNC's online Help Desk are explicitly cautioned, with a notice at the top of the request form, not to provide their EIN or SSN when making a Help Desk request.

When telemarketers download the list of telephone numbers from the DNC, the system keeps track of the area codes of the telephone numbers that are downloaded. For system auditing purposes, DNC also collects and stores the following computer system and network related information:

- Date and time when the user gained access to DNC
- Name of the domain and host from which the user gained access to the DNC site
- Internet address of the site from which the user linked directly to the DNC site
- Internet protocol (IP) address of the computer the user was using
- User's Internet browser software information
- User's computer Operating System information

[3] The Privacy Impact Assessment for Pay.gov may be found at found at http://www.fms.treas.gov/pia/paygov_pia%20.pdf.

The SpamDB collects and maintains information that is voluntarily submitted via email to spam@uce.gov. Any information included in an email message submitted to the SpamDB also is included.

The information collected in the SpamDB varies depending on what the submitter has chosen to forward to the FTC. Most often, emails submitted to the SpamDB include the body of the original email received by a consumer, along with standard email header information, which includes the email address of the consumer or entity that forwarded the email to the FTC. In addition, email header information includes sender and recipient email addresses, timestamps for each transmission between the sender and recipient, and a subject line.

Occasionally, messages forwarded to the SpamDB contain additional information, including PII such as name, address, telephone numbers, and email addresses. Typically, such information is provided by those who forward messages to the SpamDB that include their "signature line" / contact information. In addition, because information is submitted to the SpamDB via email, messages can include more sensitive information (e.g. social security or tax ID numbers, credit card numbers, and bank account numbers). However, the submission of sensitive information does not occur frequently.[4]

Finally, law enforcement users requesting access to the CSN must go through a comprehensive and secure registration process and become approved and authorized members before being given access to the information available in the system. During the law enforcement organization registration process, we collect name, mailing address, email address and contact information associated with the organization requester, organization administrator, and the approving authority within the applying organization. In addition, we also gather the static IP address range that the organization's computers will use when accessing the Internet. During the individual law enforcement user registration process, we collect the law enforcer's name, work address, telephone number, and email address, as well as a copy of their government issued ID or badge.

In addition to law enforcement users, relevant sections of CSN may be accessed by approved data contributors to periodically upload and contribute bulk consumer complaint data to the FTC. These approved data contributors will only have access to those sections of CSN that enable submission of bulk complaint data, and will not have access to the complaint data maintained in the system. Name, mailing address, email address, and phone contact information of respective and approved data contributors is collected and stored in SNS. Similar to data contributors, relevant sections of CSN may also be accessed by approved data receivers who may periodically login and download requested complaint data exported out of SNS. Currently,

---

[4] Based on a random sample of 300 messages contained within the SpamDB, approximately three percent (3%) of all submissions contain some signature line information, and approximately three tenths of one percent (0.3%) of all submissions may contain more sensitive information.

these data receivers are limited to consumer reporting agencies (CRAs), which are provided certain data pursuant to a statutory mandate, and approved CSN law enforcement members (see section 3.3 for a discussion of data sharing with CRAs). These approved data receivers will only have access to those sections of CSN that enable downloading of requested complaint data. Name, mailing address, email address, and phone contact information of prospective and approved data receivers is collected and stored in SNS.

Similar to CRC and DNC, CSN captures the following computer system and network related information for system auditing purposes:

- Date and time when the user gained access to CSN
- Name of the domain and host from which the user gained access to CSN
- Internet address of the site from which the user linked directly to the CSN site
- Internet protocol (IP) address of the computer the user was using to access CSN
- User's Internet browser software information
- User's computer Operating System information
- User's login and password

### 2.2 What are the sources of the information in SNS?

Complaints maintained in SNS are voluntarily submitted by consumers, or others acting on their behalf, to either the FTC or to our external data contributors. The major external data contributors to SNS currently include the following:

- The Internet Crime Complaint Center (IC3)
- Participating Better Business Bureaus (BBBs)
- Phonebusters
- The US Postal Inspection Service (USPIS)
- The National Fraud Information Center (NFIC)
- The Identity Theft Assistance Center (ITAC)

NOTE: a complete list of data contributors is available in the FTC's annual Consumer Sentinel Network Data Book, which can be found at www.ftc.gov/sentinel/reports.

SNS does not receive data from commercial data brokers or information resellers.

In addition, consumers who wish not to receive telemarketing calls can register their telephone numbers on the DNC, either online via the DNC website, or by calling the toll free phone numbers. Telemarketer information gathered by DNC is provided by telemarketers and sellers. Law enforcement organization and user information for access to the CSN is provided directly by the law enforcement member and their respective organization. Finally, SNS maintains the SpamDB, which includes all emails voluntarily submitted to spam@uce.gov by individuals and other entities that collect consumer complaints regarding spam emails.

### 2.3 Why is the information being collected, used, disseminated, or maintained?

The FTC collects and maintains consumer complaints to further its consumer protection mission. Unsolicited commercial emails are collected to support the FTC's law enforcement mission and to enforce the CAN-SPAM Act, including rulemaking under the Act. By collecting, maintaining, and analyzing this data, the FTC is better able to target law enforcement action, provide consumer and business education to protect the public, and identify trends in consumer fraud and law violations.

As explained above (see section 2.1), the FTC collects SSNs for two categories of complaints, identity theft complaints and complaints related to the accuracy of consumer credit reports. Consumers submitting identity theft complaints are asked to provide their SSN and other sensitive PII (e.g. account numbers, driver's license number, date of birth, etc.) in order to assist law enforcement with identity theft investigations. Consumers submitting complaints about the accuracy of their consumer credit reports are asked to provide their SSNs to enable the CRAs to accurately and efficiently match the consumer complaint to the CRA's files. SNS encrypts the SSN, and the number is not displayed when members search the system.

The FTC collects and maintains consumer telephone numbers in DNC to make them available to telemarketers for the purpose of ensuring that telemarketers do not call the numbers on the registry. In addition, all registration, verification, and deletion transaction history for individual telephone numbers is maintained to assist law enforcement action. All telemarketers' identifying information, including profile information, which includes EINs and SSNs, is maintained to assist law enforcement investigations. Law enforcement members of CSN have access to this information.

The computer system and network related information collected by SNS is used to determine the number of visitors to different sections of the respective websites including DNC, CRC, and CSN to help make the corresponding sites more useful, to help ensure the proper operation of these sites, and to help resolve Help Desk requests. SNS collects consumers' IP address information to prevent abuse and to protect the integrity and security of the system. This information is not used to track or record information about individuals.

Consumers are instructed not to provide personal information such as SSNs, credit card numbers, bank account numbers, drivers' license numbers, or health information in the comment portion of complaint forms when filing a complaint online. In addition, when a complaint is filed by a minor under the age of 13, any PII in that complaint is deleted and purged. The FTC may periodically accept complaints about minors from law enforcement partners or other third parties, when such information is needed to effectuate law enforcement investigations, and when such information is gathered and shared in a manner that complies with applicable statutes and regulations (e.g., the Children's Online Privacy Protection Act (COPPA)). In addition, the FTC will accept identity theft complaints filed by an adult on a minor's behalf. For DNC online

registration, the online registration wizard only collects consumer telephone numbers and email addresses.

For complaints submitted via Military Sentinel, the FTC allows consumers to identify their service branch, posting, and pay grade. This information is collected to enable Military Sentinel users and DOD consumer education staffers to better investigate and follow-up on complaints submitted by consumers in the armed forces.

As mentioned above (see section 2.1), the FTC also collects information from law enforcement users who request access to the CSN. This information includes contact information (e.g. name, address, etc.), IP address information, and also their login and password. The FTC collects and maintains this information to help ensure the security of the system. In addition, to foster law enforcement cooperation, contact information for CSN law enforcement users is made available to CSN members, and a list of all CSN member agencies is made available to the public.

### 2.4 How is the information collected?

The consumer complaint information gathered by the CRC is collected through the following channels:

- Interactive Voice Response (IVR) units collect data via interactive toll-free telephone sessions with consumers. Consumers may complete their transaction in the IVR or be passed to a customer service representative for further processing.
- Customer service representatives at the contact center enter or update complaints during live conversations with consumers. The customer service representatives use a complaint/identity theft entry/update interface that ensures the collection of required data elements.
- Complaints are entered directly by consumers via either the general or IDT online complaint form accessed from www.ftc.gov. The complaint forms link to the Complaint Assistant Wizard located at www.ftccomplaintassistant.gov. This is the same portal used for members accessing Military Sentinel.
- Physical mail, received by the FTC via US mail, is either mailed to or scanned and securely sent to the contractor and entered into CSN by customer service representatives using the contact center complaints/identity theft interface. Physical mail is retained onsite at the contact center for a period of one year, after which it is shredded. An electronic copy of scanned mail is attached to a complaint in the CSN system and retained under the retention schedule for complaints.

DNC registration and complaint information is collected either through the toll-free telephone numbers or the Internet site (www.donotcall.gov). Telemarketer information is gathered through the telemarketer Internet site (www.telemarketing.donotcall.gov).

The econsumer.gov site (www.econsumer.ftccomplaintassistant.gov) gathers complaints relating to cross-border e-commerce fraud and provides online complaint forms in English, Spanish, French, German, Polish, Japanese, and Korean.

These collections have been reviewed and approved by the Office of Management and Budget (OMB) (OMB Control No. 3084-0047) in accordance with the Paperwork Reduction Act.

Consumers or other entities also may forward unsolicited commercial emails to spam@uce.gov.

Law enforcement officials signing up for access to the site provide information to us about their organization and their position within their organization through the website. Signed documents confirming this information and certifying the organization's agreement to CSN's policies is done by mail, pdf by email, or fax.

Finally, for complaint data contributed by external organizations, most of the contributors send batched data using CDs, DVDs, email, or a secured Web interface. The FTC retains in a secure manner the original data contributor files for a period of 90 days after records from that file have been successfully uploaded into the SNS database. For data files received via email or Web service, the FTC encrypts the original data. At the end of this retention period, the FTC purges the original files. If the files were transmitted via CD, DVD, or similar portable media, the media is destroyed in a manner that is consistent with OMB and the National Institute of Standards and Technology (NIST) security standards.

### 2.5 How will the information be checked for accuracy and timeliness?

Consumer complaints collected by the CRC and DNC, complaints provided by data contributors, and unsolicited commercial email submitted by consumers are not checked for accuracy or validity. This information is provided voluntarily by consumers and is made available for law enforcement use and investigation (also see section 2.8, below). Telemarketer data submitted to DNC also is not checked for accuracy when it is submitted. However, telemarketers submitting that information must certify under penalty of perjury that the information they provide is true, correct, and complete. Information submitted by law enforcement organizations and their users who are requesting access to CSN is reviewed by the FTC and LM IS&GS before the application is approved and the user is granted access.

### 2.6 Is SNS using technologies in ways that the FTC has not previously employed (e.g., monitoring software, Smart Cards, etc.)? If so, how does the use of this technology affect individuals' privacy?

Yes, SNS is using new technologies in ways that the FTC has not previously employed, and is combining these with existing technologies to enhance the security and privacy of the information housed within the system.

To protect individuals' privacy, encryption technology is used to ensure information confidentiality and integrity. All sensitive data are encrypted during transmission between the SNS web portals and the end users or external systems using 128-bit Secure Socket Layer (SSL) encryption and Secure Hyper Test Transfer Protocol (HTTPS). Data downloaded or exported from SNS are encrypted and password protected. In addition, all data stored by SNS is encrypted at rest using software encryption. Importantly, all encryption and data transport protocols meet OMB and NIST standards.

In accordance with OMB and NIST standards, access to the SNS CSN portal is strictly controlled and utilizes a minimum of two authentication factors. Authentication factors include: unique user names, passwords, one-time passcodes generated by RSA SecureID tokens, approved IP address ranges, and such other factors as the FTC may determine are necessary to ensure the confidentiality and security of the system and its data.

All user access and operations are logged and logs are kept on a centralized logging server. The logs are used to audit user access and produce relevant security reports. In addition, the SNS application network perimeter is protected through advanced firewalls and Intrusion Prevention Systems (IPS).

To increase efficiency and decrease costs, the SNS system is hosted in a secure cloud environment that provides services exclusively to federal and state government entities.[5] This cloud environment has undergone an extensive Certification and Accreditation process conducted by a FedRAMP-certified third-party assessment organization. The SpamDB is in a cloud environment that is isolated from the remainder of the SNS system to mitigate any data security risks associated with spam email, which may contain viruses and other malware that can exploit security vulnerabilities. The SpamDB permits authorized CSN users to view a static image of the actual email to protect SNS and its users against any risks associated with spam email.

### 2.7 What law or regulation permits the collection of this information?

Several statutes authorize the FTC to collect and maintain consumer complaints. Section 6(a) of the FTC Act, 15 U.S.C. § 46(a), authorizes the Commission to compile information concerning and to investigate business practices in or affecting commerce, with certain exceptions. Information relating to unsolicited commercial email is collected pursuant to the FTC's law enforcement and investigatory authority under the CAN-SPAM Act of 2003, 15 U.S.C. § 7704.

In addition, the Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 note, mandates the Commission's collection of IDT complaints, and the Fair and Accurate Credit

[5]All data transfers associated with the transition to the secure cloud environment were conducted via secure, encrypted means.

Transactions Act of 2003, Pub L. 108-159, 117 Stat. 1952, requires the sharing of information with consumer reporting agencies.

Amendments to the Telemarketing Sales Rule (TSR), 16 C.F.R. Part 310, required the implementation of the National Do Not Call Registry® and collection of consumer telephone numbers and DNC-related complaints. The TSR also requires telemarketers to access the National Do Not Call Registry®. Telemarketer SSN/EIN collection is mandatory under 31 U.S.C. § 7701.

User names, password, and other system user data that is collected from CSN users accessing the secure system is collected pursuant to the Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541.

### 2.8 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Considering the type of information collected and sources of collection, the following privacy risks were identified:

- Consumers might accidentally provide sensitive PII, which is not required by SNS in the complaint's comments field, which poses a risk of identity theft.
- Consumers might accidentally provide sensitive PII in the body of their email when forwarding unsolicited commercial emails.
- Someone may try to pose as an authorized law enforcement user and try to register and obtain access to CSN, which can pose a security and privacy risk to the system.
- Data provided by consumers and/or data contributors might not be accurate, complete, or timely.
- Data provided by consumers and/or data contributors might be misused, used for a purpose not intended or contemplated by the PIA, or improperly disclosed or accessed.

**NOTE: Privacy risks and mitigation are discussed in various sections throughout this document, including sections 2.8, 3.1, 3.2, 3.3, 4.1, 4.6, 5.5, and 7.3.**

To mitigate the risk of unnecessary PII being provided by consumers, the CRC uses the Complaint Assistant Wizard, which assists consumers in filing online complaints, and which only collects the information that is relevant to a given complaint. To reduce the risks of consumers accidentally providing sensitive PII, DNC online registration and complaint forms are designed in a way that consumers can only provide required information. In addition, consumers are reminded not to provide sensitive PII in the comments field in each of these complaint forms and on econsumer.gov. We also train the staff and counselors working with consumers directly

to only collect information necessary to the specific complaint and not to collect unnecessary sensitive PII.

To mitigate the risk of unauthorized access to the CSN, CSN employs a well-defined and secure process to enable interested law enforcement organizations and their users to register and obtain access and thereby mitigate any associated security risks. This process requires users to enter a matching passcode that is specifically assigned to their law enforcement organization, submit valid and accurate information including email addresses that match their organization's email domain, and submit proper credentials, such as their badge, to verify that they indeed work for their respective organization.

As to the risk that data provided by consumers and data contributors might not be accurate, complete, or timely, it is important to note that SNS purposefully accepts self-reported consumer complaint information, and makes the process of filing complaints as easy as possible for consumers. Importantly, the information provided by consumers is well suited to the purposes for which it is collected to support the FTC's law enforcement investigations and mission – and authorized users of the data understand the benefits and risks of self-reported information.

With respect to the use and disclosure of SNS data, the FTC recognizes that there is a risk that consumers' information may be misused or disclosed for an unauthorized purpose. To mitigate the risk that this may be caused by a contractor, the FTC requires that all contractors involved with data collection and processing, as well as technical support of SNS, submit to a rigorous security clearance process, sign a non-disclosure agreement, and agree to act in accordance with specified rules of behavior.

To mitigate the risks associated with access by external law enforcement members, SNS utilizes numerous procedural controls, which include a confidentiality and data security agreement. Each member agency and each user agrees, in writing, to maintain the confidentiality and security of SNS data and only to use it for law enforcement purposes (see section 3.3 for a more detailed list of these controls). In addition to the confidentiality and data security agreement, the FTC periodically provides SNS users with training and information on how SNS data may be used and disclosed. If the FTC discloses SNS data in another manner (e.g., in response to a FOIA request or to an entity that is a subject of a complaint), it redacts PII.

In addition, as discussed throughout this document, SNS employs a significant number of layered technical controls to help prevent the misuse or improper disclosure or access of SNS data.

## 3.0 Use and Access to Data in SNS

### 3.1 How will information in SNS be used?

Both the FTC and external law enforcement members of the CSN use SNS data to accomplish their consumer protection and criminal law enforcement missions. Specifically, SNS data is used to identify potential targets for law enforcement actions. SNS data also may be used as evidence in legal proceedings and may be filed in court. In addition, SNS data may be used to help resolve consumer complaints, locate victims, respond to inquiries, provide consumer and business education, and identify trends. Law enforcement users may access an identity theft complaint in order to update it with police report information. SNS data also is used to assist with consumer redress, periodically review the effectiveness of the FTC's current consumer protection regulations, and develop consumer and business education programs and publications. Aggregate numbers compiled from SNS data also help determine the effectiveness of the FTC's consumer protection program in accordance with the Government Performance & Results Act.

Telephone numbers included in DNC are shared with telemarketers to ensure that telemarketers do not call those numbers. Information provided by telemarketers to DNC is made available to both the FTC and our CSN members for law enforcement purposes.

SNS data is used in accordance with the routine uses outlined in the FTC's Privacy Policy and Privacy Act System of Records Notices. In addition, all uses of the SNS data are both relevant and necessary to the purpose for which the data was collected. All SNS users have a level of access determined by their need-to-know, with the lowest level of access needed to perform their work.

SNS limits users' access to the features, functions and data for which they are authorized. For example, the contractors involved with data collection can only view the data which they enter or update, CPS users only can view data received through econsumer.gov, and data contributors only can access parts of the system that will allow them to contribute their data. Users cannot view Social Security Numbers. External users access the SNS applications through 128-bit SSL encryption and strong two factor authentication. The FTC also maintains audit logs of each user's activity in SNS, to make sure any data accessed can be traced for security reasons.

User name and login information collected from CSN users is used only to allow them access to the pieces of the system they have permissions for and to log which information is being accessed and by whom.

In addition, consumers' complaint information may be shared under very limited circumstances with organizations providing additional consumer counseling services. Consumers' information would only be shared with such organizations if the consumer gives prior express consent and the organization can properly protect the consumer's information..

### 3.2 Which internal entities will have access to the information?

Within FTC, SNS data is used by attorneys, investigators, paralegals, data analysts, economists, and consumer protection counselors, for the purposes outlined in section 3.1, above. All internal users have read-only access except for consumer counselors. Counselors also have the ability to enter consumer complaint information into the system and update consumer complaint records already entered, which they do when they receive updated information from the consumer complainant.

The FTC's contractor involved with the design, development, and maintenance of the system, LM IS&GS, also has access to the SNS data to maintain and support the ongoing SNS operations including web portal hosting services and call center services. For example, a call center Customer Service Representative interacts directly with consumers and records the data into the SNS system. Information confidentiality and Privacy Act requirements are specified in the service contract. In addition, SNS must undergo certification and accreditation to ensure that the security controls are properly implemented.

The FTC requires all contractors who are involved with data collection and processing, as well as technical support of SNS, to undergo a rigorous security screening and clearance process, and to sign a non-disclosure agreement.

LM IS&GS personnel who access SNS receive initial training in security awareness and agree to comply with security practices as part of their orientation. They also sign Rules of Behavior for the use of SNS systems and applications prior to being given access to those systems and applications. LM IS&GS personnel receive refresher training annually. Customer Service Representatives also receive security awareness training on sensitive information and PII handling during orientation.

The LM IS&GS personnel with access to SNS are aware of and understand the ramifications and penalties for infractions of the rules regarding privacy and data security. Any failure to comply with the Rules of Behavior is considered a security incident.

### 3.3 Which external entities will have access to the information?

As part of its consumer protection mission, the FTC shares SNS data with other law enforcement agencies (for a complete list, see http://www.ftc.gov/sentinel/members.shtml). Through the CSN, SNS data is shared with authorized local, state, federal, and international law enforcement agencies that have entered into a confidentiality and data security agreement with the FTC. This agreement requires, amongst other things, that CSN data will be accessed solely for law enforcement purposes. As noted above, IDT data is only available to those law enforcement agencies that require access. In addition, in response to specific law enforcement agency requests, the FTC will provide those agencies with data in an encrypted and password protected format, consistent with OMB and NIST standards.

As discussed previously, SNS also limits users' access to the features, functions, and data for which they are authorized. For example, the ability to extract data from SNS will be limited to local, state, and federal law enforcement agencies in the United States, Canada, and Australia, and will not be available to other foreign law enforcement users. Both the Office of International Affairs and the Office of General Counsel are consulted on all decisions regarding sharing data with foreign entities.

Certain States that have entered into a Memorandum of Understanding with the FTC may download registered consumer telephone numbers from DNC for their State and use this information to update their State-specific do not call lists.

Telemarketers with currently valid subscriptions must, in accordance with the Telemarketing Sales Rule, access and download consumer telephone numbers in their subscription at least every 31 days to ensure that they do not call those numbers.

Pursuant to the Fair and Accurate Credit Transactions Act of 2003, Pub L. 108-159, 117 Stat. 1952, and the Commission's delegation of authority located at 68 FR 46642, the FTC shares certain consumer complaints (e.g., about the accuracy of a consumer's credit report) with consumer reporting agencies (CRAs). The CRAs review the complaints, take appropriate actions, and report back to the Commission on their determinations. In addition, the CRAs will share selected complaints with consumer reporting agencies that maintain consumer files within the CRA system ("associated consumer reporting agencies" or "associated CRAs"). The CRAs will share with each associated CRA only those complaints that pertain to consumer files owned by that associated CRA, and will only share complaints with an associated CRA that has entered into a confidentiality agreement with the FTC. This information is shared in an electronic format, and is encrypted and password protected.

The FTC may be required or authorized to share complaint data with external entities in other circumstances, including in response to requests from Congress, Freedom of Information Act (FOIA) requests from private individuals or companies, requests from the media (not obtained through a FOIA request), or during litigation. Normally, in these situations, the FTC redacts all PII before providing the SNS data. Government agencies also may request SNS data for a non-law enforcement purpose. Such requests must be submitted to and approved by the Office of the General Counsel. Complaint data also may be shared with the entity about which a consumer complains in order to address the complaint. In the latter two situations, the FTC only discloses the data after receiving assurances of confidentiality from the recipients. In addition, consumers' complaint information may be shared under very limited circumstances with organizations providing additional consumer counseling services. Consumers' information would only be shared with such organizations if the consumer gives prior express consent and the organization can properly protect the consumer's information..

SNS employs a number of technical and procedural safeguards, to protect the information that is shared with external entities. See section 2.6 for a discussion of some of the technical

safeguards. In addition, as mentioned above, all CSN members are required to execute a confidentiality and data security agreement that outlines many of the SNS procedural safeguards, as follows:

- CSN data will be accessed solely for law enforcement purposes;
- any information printed, downloaded, or otherwise removed from the CSN (either in an electronic or in a printed format) must be properly protected (i.e. via NIST-approved encryption tools for electronic data, or via a locked cabinet for paper based documents);
- any data extract must be destroyed within 90 days unless its use is still required for a valid law enforcement purpose;
- CSN information must be properly destroyed;
- CSN users may only access the system from computers issued and maintained by their organizations;
- CSN users may only access CSN from their official work stations;
- CSN users may only access the system from computers with up-to-date software, including anti-virus and anti-malware programs, a firewall, and properly patched operating system and application software;
- userids and passwords must be properly protected;
- CSN access and CSN information must only be provided to individuals with a need for such access and information;
- CSN members must notify the FTC in case of a data breach;
- CSN members must ensure that their staff understand their responsibilities under the agreement; and
- CSN users must complete a mandatory online training module prior to accessing the system.

## 4.0 Notice and Access for Individuals

### 4.1 How will individuals be informed about what information is collected, and how this information is used and disclosed?

Through Privacy Act notices available on the online complaint forms and through messages and menu items for the toll-free numbers, the FTC informs consumers that the information collected is not mandatory, but that if they do not provide certain information, it may be impossible for the FTC to refer, respond to, or investigate the consumer's complaint or request. The FTC Privacy Policy also informs consumers that any information they submit in connection with a complaint is voluntary. Consumer's who choose to submit spam to the SpamDB would need to locate the email address to send submissions. This email address, spam@uce.gov, is posted on the FTC website in various places, i.e. in several press releases regarding the program, and everywhere this email address is posted, we also provide a link to the privacy policy.

The SNS programs are currently covered by three existing Privacy Act System of Records Notices (SORNs). The Privacy Act SORN corresponding to general consumer complaint collection is currently designated FTC IV-1 (consumer information system), the one corresponding to the DNC is designated FTC-IV-3 (National Do Not Call Registry® System-FTC), and an additional SORN regarding login information collected for CSN is designated FTC-VII-3 (Computer Systems User Identifiable and Access Records). The FTC's SORNs, which are published in the Federal Register, are posted and accessible online through the FTC's Privacy Act page, http://www.ftc.gov/foia/listofpaysystems.shtm and through the FTC's privacy policy. In compliance with the Privacy Act, the Internet sites and toll free phone numbers from which consumers can access the complaint forms and DNC, as well as the CSN access pages for law enforcement, contain the required notice of authority, purpose, routine uses, and whether the collection is voluntary or mandatory. They also contain links to the FTC's Privacy Policy or, in the case of the telemarketer website for DNC, a privacy notice tailored specifically to their purposes.

### 4.2 Do individuals have the opportunity and/or right to decline to provide information?

All information provided by consumers to the FTC is voluntary. Consumers may choose to submit some, all, or none of the information requested by the FTC's complaint forms. Consumers are informed during the complaint gathering process that if they do not provide certain information, it may be impossible for the FTC to refer, respond to, or investigate the consumer's complaint or request. For spam submissions, as discussed in section 4.1, consumers who choose to submit spam to the SpamDB would need to locate the email address to send submissions. This email address, spam@uce.gov, is posted on the FTC website in various places, and everywhere this email address is posted, we also provide a link to the privacy policy.

Telemarketers must set up a profile by registering an account on the DNC system before they can access telephone numbers in the National Registry. To set up a profile, telemarketers must provide organizational information. If telemarketers decline to provide organizational information, they will not be able to set up a profile or gain access to telephone number information in the National Registry.

Law enforcement users requesting access to the CSN must go through a comprehensive and secure registration process and become approved and authorized members before being given access to the information available in the system. Law enforcement organizations and their users must provide the required information (see section 2.1, above). If law enforcement users decline to provide the required information, they will not be able to complete the registration process, and they will not be given access to the CSN.

### 4.3 Do individuals have the right to consent to particular uses of the information? If so, how would an individual exercise this right?

Consumers, telemarketers, and CSN law enforcement users do not have the right to consent to particular uses of their information. They consent to their information being provided for all uses described in the applicable privacy policies. Likewise, once registered, CSN users must enter their login information each time they wish to enter the system online, or they will be denied access. Consumers can also choose to share their information with organizations that provide additional consumer counseling services. To do so, consumers would have to give express consent at the time they submit their complaint.

### 4.4 What are the procedures that allow individuals to gain access to their own information?

Consumers may request a copy of information covered by the Privacy Act, by following the FTC's Privacy Act rules and procedures, which are published in the Code of Federal Regulations at 16 C.F.R. 4.13 and highlighted in the FTC's privacy policy. Consumers may update the information they provide in a complaint by following these procedures, or by calling the CRC at 1-877-FTC-HELP or 1-877-ID-THEFT. Consumers also may access their registration information by visiting the DNC website or by calling the DNC's toll-free telephone numbers. In addition, consumers may request to remove their telephone numbers from the DNC by calling the toll-free telephone numbers from the telephone whose number they wish to remove. Telemarketers may correct their information by visiting the DNC website or by contacting the DNC Help Desk. CSN users can access or change their identifying information or passwords by loging into the system and changing the information in their profile.

### 4.5 If no formal procedure for individuals to access and/or correct their own information is provided, what alternatives are available to the individual?

Not applicable.

### 4.6 Discuss the privacy risks associated with the process of providing individuals access to their own records and how those risks are mitigated.

Requests by individuals for access to SNS information are reviewed and evaluated by the FTC's FOIA office, in accordance with the FTC's Privacy Act rules and procedures, which are published in the Code of Federal Regulations at 16 C.F.R. 4.13 (see section 4.4, above). In this regard, privacy risks inherent in the process are managed by the FTC's FOIA Office.

Requests made to the CRC by consumers wishing to update information they submitted are processed by CRC staff. To mitigate the risk that a consumer's information might be updated or shared with an unauthorized third party, the CRC requires callers to provide the unique reference number associated with the consumer's complaint, as well as other identifying details. Each

complaint in CSN is assigned a unique reference number, which is provided to the consumer when a complaint is filed.

In addition, consumers may access information related to their DNC registration by visiting the DNC website, or by calling the toll-free DNC telephone number. To mitigate the risk that a consumer's information might be altered or shared with an unauthorized third party, the DNC website employs a multi-step process, which includes the delivery of a confirmation email. The website may only be used to register a telephone number, verify a registration, or file a complaint. Consumers cannot remove or delete a registration via the website. Consumers who use the toll-free DNC telephone number must call from the telephone number that is registered to access or change any DNC information.

## 5.0 Website Privacy Issues

### 5.1 Describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon).

For system auditing purpose, SNS collects and stores the following computer system and network related information on each SNS website, including consumersentinel.gov, donotcall.gov, econsumer.gov, and ftccomplaintassistant.gov:

- Date and time when the user gained access to SNS
- Name of the domain and host from which the user gained access to SNS
- Internet address of the site from which the user linked directly to the SNS websites
- Internet protocol (IP) address of the computer the user was using
- User's web browser software information
- User's computer Operating System information

The computer system and network related information is used to determine the number of visitors to different sections of the SNS websites, to help make the websites more useful, to help ensure the proper operation of the websites, and to help resolve helpdesk requests. This information is not used to track or record information about individuals.

SNS websites, including consumersentinel.gov, donotcall.gov, econsumer.gov, and ftccomplaintassistant.gov, do not use persistent "cookies" or tracking mechanisms that collect PII. All of these websites, except for econsumer.gov, do use session cookies on the site to collect a visitor's IP address and the date and time of the visit. Session cookies are temporary files that are erased when a user closes all browsers. The website uses these session cookies so that telemarketers, sellers, law enforcement agencies and other entities accessing the site can move from one secure web page to another without having to log in to each page. Session

cookies are mandatory to ensure the proper functioning of our site. Users may not be able to use the SNS websites if they decline to accept session cookies. In addition, consumersentinel.gov also users a RSA authentication cookie. Because of the high level of security required to protect the information available in Consumer Sentinel, these cookies are required to prevent members from having to log on at each separate page, severely hampering the usability of the system for our law enforcement members.

**5.2 If a persistent tracking technology is used, ensure certain issues are addressed.**

SNS does not use persistent cookies, web beacons, Adobe flash cookies, or other persistent tracking devices on the system websites.

**5.3 If personal information is collected through a website, page, or online form accessible through the Internet, is appropriate encryption used? If not, explain.**

SNS uses 128-bit SSL encryption when personal information is collected through a website, page, or online form. Encryption also is applied to personal information, collected from consumers, telemarketers and law enforcement agencies, which is stored in the SNS database. No personal information is collected for the SpamDB through the website or by an online form.

**5.4 Explain how the public will be notified of the Privacy Policy.**

Privacy policy information is made available to the public via a hyperlink on every SNS website as well as on the ftc.gov website. The SNS privacy policy is machine-readable (i.e. P3P compliant), and handicap accessible pursuant to Section 508 of the Rehabilitation Act.

**5.5 Considering any website or Internet issues, please describe any privacy risks identified and how they have been mitigated.**

The FTC has identified privacy risks associated with SNS and has taken steps to mitigate those risks. With respect to the collection of data, the identified risks are:

- Consumers might not understand how their information will be used
- SNS might collect more information than is required (e.g., consumers provide SSNs on the general complaint form when not needed)

**NOTE: Privacy risks and mitigation are discussed in various sections throughout this document, including sections 2.8, 3.1, 3.2, 3.3, 4.1, 4.6, 5.5, and 7.3.**

To address these risks, SNS provides notices (on the online complaint forms and through telephone counselors) about how consumers' information will be used. On the online complaint

forms, SNS provides a link to the FTC's Privacy Policy. Social Security Numbers, if provided, are encrypted when stored in SNS. SNS also explains on the general complaint form that a Social Security Number should be provided only for certain types of complaints.

### 5.6 If the website will collect personal information from children under 13, or be directed at such children, explain how it will comply with the Children's Online Privacy Protection Act (COPPA).

SNS websites are not directed to children under the age of 13, and if an individual lodges a complaint and indicates that he/she is under the age of 13, SNS deletes and purges any PII in that complaint. However, SNS websites accept identity theft complaints filed on behalf of a minor by an adult.

## 6.0 Security of Information in SNS

### 6.1 Are all IT security requirements and procedures required by federal law being followed to ensure that information is appropriately secured?

The FTC follows all applicable FISMA requirements to ensure that information in SNS is appropriately secured.

### 6.2 Has a Certification & Accreditation (C&A) been completed for the system or systems supporting the program?

A FedRAMP-certified third-party assessment organization conducted a Certification and Accreditation for the SNS. The C&A was completed in August 2012.

### 6.3 Has a risk assessment been conducted on SNS?

As part of the SNS C&A process, a Risk Assessment was conducted on SNS. Appropriate security controls have been identified and implemented to protect against the identified risk.

### 6.4 Does SNS employ technology that may raise privacy concerns? If so, please discuss its implementation.

Yes. The SpamDB email preview feature and back-up Simple Mail Transfer Protocol (SMTP) relay are hosted in the Amazon Web Services (AWS) Cloud, which incorporates highly restricted access controls and encryption technology are implemented in the AWS to protect SpamDB data. These security features, together with isolating the SpamDB from the remainder of the SNS system mitigate any data security risks associated with spam email, which may contain viruses and other malware that can exploit security vulnerabilities. The SpamDB permits authorized CSN users to view a static image of the actual email to protect SNS and its

users against any risks associated with spam email.

### 6.5 What procedures are in place to determine which users may access the system and are they documented?

Access to the SNS CSN portal is role-based for all SNS users, including FTC staff, external law enforcement members, call center staff, data providers, and data receivers. In accordance with OMB and NIST standards, access to the SNS CSN portal is strictly controlled and uses a minimum of two authentication factors. Authentication factors include unique user names, passwords, one-time passcodes generated by RSA SecureID tokens, approved IP address ranges, and such other factors as the FTC may determine necessary to secure the system and its data.

Data contributors and data receivers are also authenticated if they access SNS to either contribute or receive data. Their access is restricted to only uploading or downloading of data.

### 6.6 Describe what privacy training is provided to users either generally or specifically relevant to the program or system.

The LM IS&GS personnel managing or accessing the SNS systems have received initial training in security awareness and accepted security practices as part of their orientation and sign Rules of Behavior for the use of systems and applications prior to their being given access to those systems and applications. LM IS&GS personnel receive refresher training annually.

Consumer Service Representatives from the CRC also receive security awareness training on sensitive information and PII handling during orientation and receive annual training.

For SNS CSN users, a mandatory online training course on PII data handling must be taken prior to first use and repeated annually. Training record information is kept online as part of the user profile.

### 6.7 What auditing measures and technical safeguards are in place to prevent the misuse of data?

The following in-place auditing measures and technical safeguards are applied to prevent misuse of data. These controls include:

- Authenticator/Password Management – Application and monitoring of initial distribution, composition, history, compromise, and change of default authenticators.
- Account Management – Application and monitoring of account establishment, activation, modification, disabling, removal (including unnecessary/defunct accounts) and review.
- Access Enforcement – Application and monitoring of access privileges.
- Least Privilege – Access to SNS data is limited to data necessary for specific user to perform his/her specific function..

- Unsuccessful Login Attempts – System automatically locks the account when the maximum number of unsuccessful attempts is exceeded.
- Audit logs are reviewed for technical and administrative errors.

Privacy risks associated with unauthorized disclosure of information are mitigated through implementation of technical controls associated with need-to-know and least privilege, ensuring that users have no more access to data and no more administrative rights than are required to affect their official duties. In addition, deterrent controls in the form of warning banners, rules of behavior, confidentiality agreements and auditing are in place. Procedures are in place to disable and delete user accounts at the end of use.

### 6.8 Questions regarding the security of the system

Questions regarding the security of the system should be directed to the FTC's Chief Information Security Officer.

## 7.0 Data Retention

### 7.1 For what period of time will SNS data be maintained?

FTC has submitted to the National Archives and Records Administration (NARA) and NARA has approved a comprehensive records disposition schedule that replaces FTC's prior records schedules and schedules previously unscheduled items including electronic systems such as SNS. SNS maintains all complaints filed by consumers (including identity theft and DNC) for a period of 5 years. The SpamDB maintains all submissions sent by consumers for a period of 3 years. Twice a year, all complaint and SpamDB records older than the applicable retention period are deleted, unless a CSN member indicates that a record must be retained for litigation purposes. In those instances, the record will be maintained until the litigation hold is lifted. Consumer telephone numbers remain on the National Do Not Call Registry until the consumer deletes the number. Telephone numbers deleted from the Registry remain in the SNS system to support investigations by CSN law enforcement members in the United States, Canada, and Australia of violations of the Telemarketing Sales Rule. See Section 1.2. Data contributor media is destroyed 90 days after information on the media has been imported into SNS. Original copies of letters and correspondence from consumers received via the mail are retained for one year, and then destroyed. All other records are retained for a period of 30 days. Examples of these records include consumer requests for information, consumer calls referred to other entities, and solicitations. These records are deleted every 60 days.

### 7.2 What are the plans for destruction or disposal of the information?

All SNS information that is subject to disposal (see Section 7.1) is destroyed in accordance with OMB and NIST guidelines.

### 7.3 Describe any privacy risks identified in the data retention and disposal of the information, and describe how these risks have been mitigated.

To mitigate the risks of unauthorized access or sabotage of privacy data stored in SNS, data encryption technology is employed to secure data in the SNS system. See Section 2.8 for more information on privacy risks identified in the data retention and how the risks have been mitigated. Media received from SNS data contributors is securely stored for 90 days after information on the media has been imported into SNS and is then destroyed in accordance with OMB and NIST guidelines. Data is deleted in a manner that makes it impossible to recover.

## 8.0 Privacy Act

### 8.1 Will the data in the system be retrieved by a personal identifier?

Yes. Consumer complaint data can be retrieved by the following fields:

- Consumer name
- Street address
- EIN or SSN
- Telephone number
- Email address
- Unique FTC reference number

Telemarketer information can be retrieved by the following fields:

- Organization name
- Street address
- EIN or SSN
- Telephone number
- First name or Last name
- Email address

SpamDB submissions can be retrieved by the following fields:

- Submitter's email address
- Personal identifiers in the body of the email may be searchable by keyword search

CSN member information can be retrieved by:

- Member first name or last name
- Organization name

**NOTE: Telemarketer business entities are not covered by the Privacy Act.**

For two categories of consumer complaints -- identity theft-related complaints and complaints related to the accuracy of the consumer's credit report -- SNS allows the consumer to provide a Social Security Number. SNS encrypts the SSN, and the number is not displayed when users search the system. However, the system allows users to search for complaints by specific SSN.

### 8.2 Is the system covered by an existing Privacy Act System of Records notice (SORN)?

The Privacy Act SORN corresponding to general consumer complaint collection is currently designated FTC IV-1 (consumer complaints generally). The FTC's SORNs, which are published in the Federal Register, are posted and accessible online through the FTC's Privacy Act page, http://www.ftc.gov/foia/listofpaysystems.shtm. In compliance with the Privacy Act, the Internet sites from which consumers can access the general and IDT complaint forms contain the required notice of authority, purpose, routine uses, and whether the collection is voluntary or mandatory. They also contain links to the FTC's Privacy Policy.

The DNC is currently covered by one Privacy Act SORN, which is currently designated FTC-IV-3 (National Do Not Call Registry® System-FTC), is published in the Federal Register, and is posted and accessible online through the FTC's Privacy Act page linked to above. In compliance with the Privacy Act, the Internet sites and toll-free numbers from which consumers can access DNC contain the required notice of authority, purpose, routine uses, and whether the collection is voluntary or mandatory. Both the consumer and telemarketer Internet sites also contain links to the FTC's Privacy Policy.

The login information collected for CSN is covered by one Privacy Act SORN, which is currently designated FTC-VII-3 (Computer Systems User Identifiable and Access Records), is published in the Federal Register, and is posted and accessible online through the FTC's Privacy Act page, link found above. In compliance with the Privacy Act, the Consumer Sentinel website from which this information is collected contains the required notice of authority, purpose, routine uses, and whether the collection is voluntary or mandatory. The website also contains a link to the FTC's Privacy Policy.

## 9.0 Privacy Policy

The collection, use, and disclosure of SNS information has been reviewed to ensure consistency with the FTC's Privacy Policy.

## 10.0 Approval and Signatures

Prepared for the business owners of the system by:

**Federal Trade Commission**

David Torok
Associate Director
Division of Planning and Information
Bureau of Consumer Protection

Alexander C. Tang, Attorney
Chief Information Security Officer
Office of the General Counsel

Peter Miller
Acting Chief Privacy Officer

Jeffrey Smith
Information Assurance Manager

Jeff Nakrin
Director, Records and Filings Office

Approved:

Jeff Huskey
Chief Information Officer

Date:

**Lockheed Martin**

Murali Thirukkonda
Program Manager

Jason Ni
Information Systems Security Officer