Federal Trade Commission
Privacy Impact Assessment

Sentinel Network Services (SNS)

Reviewed and Updated

March 2023

Table of Contents

1 System Overview 3
2 Data Type, Sources, and Use 9
3 Data Access and Sharing 17
4 Notice and Consent 21
5 Data Accuracy and Security 24
6 Data Retention and Disposal 25
7 Website Privacy Evaluation 26
8 Privacy Risks and Evaluation 27

1 System Overview

1.1 Describe the project/system and its purpose.

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; to collect complaints about calls that consumers receive; to assist telemarketers in complying with regulations; and to 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 the FTC in achieving its consumer protection mission.

Consumer complaint information received by the FTC is 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. Likewise, civil and criminal law enforcement members are able to access, analyze and extract data from CSN, which also provides a host of other investigatory tools.

In response to the White House Executive Order entitled "Improving the Security of Consumer Financial Transactions," released on October 17, 2014, BCP provides the website IdentityTheft.gov (IDT), which lets consumers who have experienced identity theft create a customized recovery plan based on their specific situation. The website allows consumers to enter identity theft complaint information, create an identity theft report, and then provides consumers with a personalized checklist of steps and tools to remediate the identity theft. The FTC encourages consumers to file a complaint if they feel they have been the victim of fraud, identity theft, or other unfair or deceptive business practices. Consumers can file their complaints online, using the self-service websites ReportFraud.ftc.gov and IdentityTheft.gov, or by calling the FTC's Consumer Response Center. ReportFraud.ftc.gov (Report Fraud or RF) collects public complaints from consumers about identity fraud and other fraud complaints. Consumers can also

use Econsumer.gov, an initiative of the International Consumer Protection and Enforcement Network (ICPEN). Using Econsumer.gov, consumers can report international scams and learn about other steps they can take to combat fraud.

BCP's DNC, CRC, CSN, IDT, RF and Econsumer programs are collectively referred to as Sentinel Network Services (SNS). The FTC has contracted with Leidos (formerly Lockheed Martin Information Systems & Global Services) to implement, maintain, and operate SNS. 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 Consumer Response and Operations (DCRO).

A. Consumer Response Center (CRC)

The CRC gathers, processes, and updates consumer information via telephone-based services and Internet-based complaint forms. 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
- Teletypewriter (TTY) for hearing impaired persons
- Live telephone conversations with customer service representatives

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 report, and request or receive consumer education materials.

Consumers may also file complaints directly from their computers and mobile devices using the online ReportFraud portal, which asks consumers to answer a series of questions organized into a few simple steps. The portal can be accessed from the URLs www.ReportFraud.ftc.gov and www.ftc.gov/complaint. Based on the consumer's submission the portal will recommend next steps, including details for reversing fraudulent transactions, and allow users to see how scams are impacting their specific community. Additionally, the self-service complaint capability allows ReportFraud.ftc.gov users to provide updated information for their complaint via ReportFraud.ftc.gov. Consumers who file complaints online in Spanish using their computers also have access to a web chat feature if they need technical assistance. This web chat feature is not currently available to consumers using mobile devices. The ReportFraud.ftc.gov website also uses an automated Chatbot service to assist consumers and to quickly connect with the answers they need when filing a complaint. The Chatbot service is available 24 hours a day, seven days a week.

Consumers with cross-border e-commerce complaints[1] may file an online complaint at www.econsumer.gov, which offers cross-border consumer protection information and an additional separate online cross-border complaint form. All information on econsumer.gov, including the complaint form, is available in English, Spanish, French, German, Polish, Japanese, Korean, and Turkish. Cross-border e-commerce complaints received from consumers through the econsumer.gov complaint form are automatically entered into CSN.

Consumers may also contact the CRC through postal mail. Physical mail received by the FTC is scanned by the agency's offsite mailroom digitization vendor and then sent to the CRC for processing. It is then reviewed and entered into the Consumer Sentinel Network (CSN) by customer service representatives using the contact center complaint interface.

As of September 2021, consumers have filed nearly 2,878,610 identity theft, fraud, and other complaints with the FTC. Approximately 86% of those complaints (2,609,208) were submitted online.

B. National Do Not Call Registry® (DNC)

The 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 in the DNC system 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 TTY access.

Telemarketers may access DNC through the Internet site www.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 DNC 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 the DNC registry, 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

[1] Cross-border complaints are those where the consumer's reported country of residence is different from the country where the consumer reports the company is located.

members can access information about the registration, verification, and deletion of 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. Consumer complaint data received through DNC is made available to law enforcement on the CSN. In addition, alleged violations are reported every weekday on the Do Not Call Reported Calls Data webpage. This data contains the telephone number that made the unwanted call, date and time the call was made, the subject matter of the call, whether the call was reported to be a robocall, and the complainant's city and state.

C. Consumer Sentinel Network (CSN)

CSN, which is located at www.consumersentinel.gov, is the website through which local, state, federal, and international law enforcement agencies access complaints collected by the CRC directly from consumers or complaints collected by other entities and forwarded to the FTC. Included within CSN is the IDT Data Clearinghouse, which is the nation's repository of identity theft complaints, gathered through the Identity Theft Portal. Identity theft complaints are only available to those law enforcement agencies that request, and are approved for, access to that data.

Law enforcement authorities that are members of www.econsumer.gov also can access a subset of the complaints housed in CSN. The www.econsumer.gov site is an initiative of the International Consumer Protection and Enforcement Network (ICPEN). ICPEN is a network of governmental organizations in the enforcement of fair trade practice laws and other consumer protection activities. Through the www.econsumer.gov website, consumers can file complaints focusing on e-commerce and fraud. Those complaints are housed in CSN, and members of econsumer.gov are able to access the complaints received through econsumer.gov. Members of econsumer.gov also can access cross-border complaints in CSN filed through the FTC's CRC (either online via ReportFraud.ftc.gov or over the phone) or obtained from external data contributors that have agreed to share complaints with econsumer members. The econsumer members will receive these complaints with all consumer PII redacted, except for the consumers' country of residence (if it is reported). If an econsumer member requires the consumers' PII to support an ongoing investigation or enforcement action, they can apply directly to the FTC to obtain the complaints containing that information.[2]

Authorized users access the CSN through a secure, password-protected internet site that uses two-factor authentication. CSN users' access to the various subsets of data in the system is based on the access requested by and approvals granted to the organization to which they belong. For example, certain Canadian law enforcement organizations have access to general fraud complaints but not identity theft complaints.

[2] The FTC make determinations about releasing the requested information pursuant to existing procedures set out by the Commission's delegation of authority effective March 14, 1997, 62 Fed. Reg. 15185, and the re-delegation by the Director of the Bureau of Consumer Protection dated May 22, 1997.

Authorized CSN users may search the complaint database by company or suspect name, address, telephone number, consumer location, type of scam or identity theft, etc. As of 2021, CSN served over 2,600 law enforcement users around the world that have signed appropriate confidentiality agreements restricting their use and disclosure of CSN data to law enforcement purposes.

Information from the CSN system may be compared to existing matter information within the FTC Redress Enforcement Database (RED) to determine whether any relationships may exist involving likely recidivists. An automated search between the two systems is performed to determine if relevant matter-related words or concepts appear in CSN that may overlap with data in CSN; if a match appears, a notice is emailed to the FTC staff person working on that particular matter. There is no direct connection between CSN and RED; for more information about RED, refer to the Redress Enforcement Database PIA.[3]

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 inspecial investigations

D. Identity Theft Portal (IDT)

IDT, accessed at www.IdentityTheft.gov, allows consumers to file their identity theft complaints, receive identity theft educational information, and use advanced functionality to assist with their recovery and remediation. IDT offers secure, self-service capabilities that provide consumers with a personalized identity theft recovery plan and the opportunity to notify the Internal Revenue Service (IRS) directly of tax-related ID theft. The portal provides consumers with customized recovery steps and tools to track their actions in remediating identity theft.

After filing an identity theft complaint, consumers are provided with the option to create an account on IDT. Consumers who set up an account on IDT access it through the secure, password-protected website with two-factor authentication. To create an account, consumers are sent a temporary password (which is active for 24 hours) to their previously entered email address. Consumers log in using their email address and the temporary password, at which time they are prompted to create a permanent password for future use. At that point, a one-time passcode is delivered to consumers' phones. Consumers must use this temporary passcode, which is active for five minutes, to gain access to their IDT account. Moreover, each time consumers access their IDT account, a one-time passcode is delivered to their phone that must be

[3] All FTC Privacy Impact Assessments are available online.

entered along with their email address and password.

Consumers can use IDT to:

- File an identity theft complaint and receive an IDT report
- Obtain a personalized checklist of steps they should take to review
- Utilize a personalized dashboard to track their progress and suggest additional action steps based on an updated complaint information
- Access and update their IDT report as often as necessary
- Automatically generate prefilled letters and forms, based on their complaint information, that consumers can send to CRAs, government agencies, and businesses to resolve their incidents of identity theft
- Electronically submit an Identity Theft Affidavit (IRS Form 14039) to the IRS

For some SNS websites, including www.donotcall.gov, www.econsumer.gov, and ReportFraud.ftc.gov, the FTC participates in the General Service Administration's (GSA's) Federal Digital Analytics Program, which uses a Federal government-specific version of Google Analytics Premium. More information on that program is accessible at https://digital.gov/services/dap/common-questions-about-dap-faq/. In addition to Google Analytics, the FTC also uses the Microsoft Application Insights (MAI) feature, which provides extensible application performance management and monitoring of live web apps. MAI is used to automatically detect performance anomalies, diagnose issues using powerful analytics tools, analyze SNS application user behavior, and generally improve application performance and usability. The metrics collected are based on the website usage and performance, not on the user supplying the information. This includes the logical location of the where the user's requests come from (IP address, city, state, country), the user's device, operating system, browser, request performance (request duration/average duration), request failures (status code, exceptions, user's input that caused the exception). This data is used to support and improve application development and address performance issues.

The Identity Theft Report Verification Portal allows the three national Credit Reporting Agencies (CRAs)—Experian, Equifax, and TransUnion—to verify the validity of potentially fraudulent identity theft reports purportedly generated from IdentityTheft.gov. This secure online portal permits a limited number of CRA employees to check whether a questionable report was filed on IdentityTheft.gov, based on information contained in SNS. Following a two-factor authentication protocol, the portal requires the CRA employee to enter the consumer's first name, last name, and the identity theft (IDT) report number, as they appear on the IDT report provided by the consumer to the CRA. After it searches SNS for this information, the portal informs the CRA user whether there is a full match, partial match, or no match. The portal does not display nor verify the content of the IDT report, and it does not provide any other consumer data. The verification portal is limited to individual searches.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

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 Executive Order 13681, Improving the Security of Consumer Financial Transactions, requires various government agencies to consolidate identity theft resources onto IdentityTheft.gov wherever possible, and to enhance the functionality of IdentityTheft.gov, including by coordinating with the credit bureaus to streamline the reporting and remediation process with the credit bureau's systems to the extent feasible.

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 Modernization Act of 2014 (FISMA), 44 U.S.C. § 3551 et seq.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[4] may be collected or maintained in the system/project. Check <u>all</u> that apply.

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 and IDT collect such information directly from consumers or from their guardians or others acting on their behalf. The information may be submitted by using the CRC's online ReportFraud portal found at ReportFraud.ftc.gov or www.ftc.gov/complaint, developing a personalized identity theft recovery plan at www.IdentityTheft.gov, or by calling or writing to the CRC. Consumers may also submit similar information through the separate complaint form found at econsumer.gov. The personal information provided to and collected by SNS are included in the table below.

[4] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.

- ☒ Full Name
- ☒ Date of Birth
- ☒ Home Address[5]
- ☒ Phone Number(s)
- ☐ Place of Birth
- ☒ Age (range)
- ☐ Race/ethnicity
- ☐ Alias
- ☐ Sex
- ☒ Email Address
- ☐ Work Address
- ☒ Taxpayer ID
- ☒ Credit Card Number
- ☐ Facsimile Number
- ☐ Medical Information
- ☐ Education Records
- ☒ Social Security Number
- ☐ Mother's Maiden Name
- ☐ Biometric Identifiers (e.g., fingerprint, voiceprint)
- ☐ Audio Recordings
- ☐ Photographic Identifiers (e.g., image, x-ray, video)
- ☐ Certificates (e.g., birth, death, marriage, etc.)
- ☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)
- ☐ Vehicle Identifiers (e.g., license plates)
- ☒ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)
- ☒ Geolocation Information
- ☐ Passport Number
- ☒ User ID
- ☐ Internet Cookie Containing PII
- ☐ Employment Status, History, or Information
- ☐ Employee Identification Number (EIN)
- ☐ Salary
- ☒ Military Status/Records/ ID Number
- ☒ IP/MAC Address
- ☐ Investigation Report or Database
- ☐ Driver's License/State ID Number (or foreign country equivalent)
- ☒ Other *(Please Specify)*: See description below

Additional PII elements may include: address of victim at time of identity theft (if different than current address), relationship to suspect (only for identity theft complaints), free-form description of consumer's issue(s), and steps taken in remediating their identity theft problem, login and password information (only for identity theft complaints). A complainant's zip code and complaint reference number may also be included.

Consumers submitting complaints about the accuracy of their credit reports are encouraged to submit their complaints to the Consumer Financial Protection Bureau (CFPB), and those filing their complaints online are directed to the appropriate form at that agency. SNS 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 the 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 consumers submit their entire identity theft complaint by phone, but would like to print a copy of a report of their complaint to provide to law enforcement, the CRC customer service representative will start the IDT account creation process by generating a temporary password that will be sent to the consumers' email address. Consumers will access their IDT account online using a two-factor authentication process and will be prompted to create a permanent password. They then will be able to print their report from the secure dashboard.

[5] As the consumer begins to type in his/her address, an address auto-completion application verifies and validates the consumer's address, listing possible responses. In performing this function, this application does not collect or have access to consumer information in the SNS database.

When consumers' complaints contain information about an individual, the CRC and IDT may collect the following personal information about the individual about whom the consumers are 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)
- Individual's relationship to consumer (only for identity theft complaints)
- Method that the 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 complaint form, consumers who identify themselves as associated with the military may provide their service branch, posting, status, and whether they are an officer or enlisted member.

To help victims of scams reverse high dollar, fraudulent banking transactions, ReportFraud.ftc.gov may also collect complaint data with useful banking data fields and facilitate data transfer to the FBI Recovery Asset Team (RAT) for investigation.

If consumers opt to submit an Identity Theft Affidavit (IRS Form 14039) electronically to the IRS when visiting IDT, the following additional information may be requested to complete the affidavit:

- Taxpayer Identification Number (Social Security Number)[6]
- Tax year(s) where identity theft occurred
- Last year a tax return was filed
- Preferred contact language
- Preferred contact time
- Mailing address and name used on last filed tax return (if changed)
- Copy of IRS notice or letter number (if received)
- If affidavit is being filed out by representative on behalf on consumer, their relationship to the consumer

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

- Name of the domain and host from which the consumer gained access to the online complaint forms
- Answers or responses provided by consumers to the questions presented by the online ReportFraud portal or the IVR while gathering their complaints
- Date and time when the consumer's complaint or questions are submitted or updated[7]

[6] Consumers have the option to submit an Identity Theft Affidavit (Form 14039) electronically to the IRS when they visit www.IdentityTheft.gov. If consumers opt to fill out the affidavit, they will need to provide their SSN. SSNs collected for the purpose of filing an affidavit with the IRS will be deleted from SNS within two business days after the IRS confirms receipt of the affidavit, and in any event, no later than 15 days after the consumer submits it to the FTC.

[7] Only the first two bullets on this list – answers provided by consumers and date and time when a consumer submits or

- Duration of any web chat session
- Transcripts of any web chat sessions[8]
- User's Internet browser software information
- Time and date of login to IDT account

The source Internet Protocol (IP) address of the computer used by the consumer when submitting an Identity Theft complaint is collected to identify fraudulent, repetitive, or erroneous submissions.

Consumers with technical and navigation questions on IdentityTheft.gov can click on a web chat icon labeled: "Having trouble categorizing your complaint? Click here to chat with tech support [hours are listed]." Consumers then receive a dialogue box that prompts them to put their first name and up to 250 characters of alphanumeric text to describe their technical issue. The consumer's first name and description of their technical issue is collected to facilitate a professional interaction with the customer service representative and to aid in resolving the consumer's issue. This information, along with a transcript of the chat, date, and duration of the chat, are maintained for auditing, QA, and billing purposes only.

SNS also includes consumer complaint data collected and forwarded to the FTC by external data contributors. 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 type 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 containing a single-use, limited duration link to confirm the DNC registration information. Importantly, the DNC registry uses a secure hash algorithm to maintain the security of consumers' email address information. For consumers who call 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 sensitive PII such as their SSNs. Any such information is redacted and not retained. Consumers are also asked to answer the following four questions:

- Have you done any business with this company in the last 18 months or contacted

updates his/her complaint or questions – are directly linked to the complaint information stored in SNS.

[8] The content of log chat sessions are collected and retained for 60 days for auditing, accounting, and quality assurance purposes. The web chats prompt users not to share personal information and automatically redacts SSN.

them in the last 3 months?
- Was this a pre-recorded message?
- Have you asked this company to stop calling you?
- Did you receive a phone call or mobile text message?[9]

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, the federal government payment processor operated by the US Department of the Treasury, and is not shared with the FTC.[10]

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. If an EIN or SSN is provided, it is redacted.

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 and security purposes, DNC also collects and stores certain computer system and network related information. This information, which typically is collected for any website that maintains logs, is needed to protect the security of the site and monitor traffic patterns, including threat indicators of attacks on the site. It includes the following:

- 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

Law enforcement users requesting access to the CSN must go through a comprehensive and secure registration process and become approved and authorized CSN members before being given access to the information available in the system. During the law enforcement organization registration process, the FTC collects 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, the FTC also gathers the static IP address range that the organization's computers will use when accessing the Internet. Law enforcement users' access to the CSN is restricted to the IP address range provided at registration in order to reduce the risk of unauthorized access. During the individual law enforcement user registration process, the FTC collects the law enforcer's name, work address, telephone number, and email address, as well as a copy of their government issued ID or badge.

[9] If the consumer indicates that they received a text message, they are redirected to ReportFraud to file their complaint.
[10] For more information, see Pay.gov Privacy Impact Assessment.

In addition to law enforcement users, relevant sections of CSN may be accessed by approved data contributors periodically to upload and contribute bulk consumer complaint data to the FTC. These approved data contributors only have access to those sections of CSN that enable submission of bulk complaint data and do not have access to the complaint data maintained in the system. Name, mailing address, email address, and phone contact information of prospective 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 that has been exported out of SNS. This is a manual intervention process; access to this feature is limited and information is not made available for download without prior review and approval by the FTC.

Similar to CRC and DNC, CSN captures the certain computer system- and network-related information for security and system auditing purposes. This information, which typically is collected for any website that maintains logs, is needed to protect the security of the site and monitor traffic patterns, including threat indicators of attacks on the site. It includes the following:

- 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 types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

The customer service representative with whom the consumer chats and the automated Chatbot are trained to provide information about technical assistance and to avoid substantive advice or assistance that could lead to a consumer providing sensitive PII. Consumers are randomly selected to participate in a customer satisfaction survey after both the telephone and online complaint process. Participation is strictly voluntary, and no personal information is collected in these surveys. The FTC uses aggregate reports of the findings and any specific comments that consumers chose to provide to improve the quality of FTC services.

2.3 What is the purpose for collection of the information listed above?

The FTC collects and maintains consumer complaints to further its consumer protection mission. 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.

The FTC collects and maintains consumer telephone numbers in DNC to make them available to

telemarketers to ensure 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 Google Analytics information collected by SNS is used to determine the number of visitors to different sections of the respective websites – including DNC, ReportFraud.ftc.gov, IDT and econsumer.gov – to help make the corresponding sites more useful, to help ensure the proper operation of these sites, and to help resolve Help Desk requests.[11] SNS also collects consumers' IP address information and other session or user data to protect the integrity and security of the system and identify fraudulent, repetitive, or erroneous submissions. SNS also uses analytical data collected by Microsoft Application Insights (MAI) to monitor, in real time, web traffic to all SNS sites, identify application errors, gather data on the usage, and apply fixes more quickly and efficiently. In addition to supporting application development and improvement, the information gained through MAI allows the FTC to evaluate performance metrics and assess the health of the SNS websites.

Information is collected through the live web chat and automated Chatbot features for the purpose of improving the consumers' experience, to provide technical assistance regarding complaints being filed, and to better tailor the online ReportFraud.ftc.gov portal to meet consumers' needs. A minimum amount of information is collected to meet this objective.

For complaints submitted by consumers identifying themselves as members of or dependents to members of the military, the FTC allows consumers to identify their service branch, posting, status, and whether they are an officer or enlisted. This information enables CSN law enforcement members to better investigate and follow-up on complaints submitted by, and fraud directed at, consumers in the armed forces.

As previously mentioned, 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 all CSN members, and a list of all CSN member agencies is made available to the public.

When a user opts to submit an Identity Theft Affidavit (Form 14039) to the IRS through IDT, the FTC collects personal information to complete the form. This information is submitted to the IRS via the IRS Secure Data Transfer System.[12]

The Identity Theft Report Verification Portal allows CRAs to verify whether questionable consumer IDT reports were generated in IdentityTheft.gov.

---

[11] For more information on how Google Analytics collects aggregated and anonymized information to analyze web traffic on the SNS sites, see https://digital.gov/services/dap/common- questions-about-dap-faq/.

[12] For more information about how the IRS handles PII, see the IRS Privacy Policy.

In certain cases, SNS provides banking information from ReportFraud.ftc.gov to the FBI Recovery Asset Team (RAT) to assist victims in reversing high value fraudulent transactions.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	*Type of Data Provided & How It Is Collected*
Members of the Public (Consumers)	Complaints maintained in SNS are voluntarily submitted by consumers (or others acting on their behalf) to either the FTC or to the FTC's external data contributors. Consumer complaint information gathered by the CRC is collected through the following channels: • 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 the Online ReportFraud.ftc.gov portal, which may be accessed from www.ftc.gov or www.IdentityTheft.gov using computers or mobile devices. • Voluntary consumer surveys hosted by ForeSee and the CFI Group.[13] • Live Web Chat and Chatbot software by consumers entering information about technical issues. • Consumers may also contact the FTC with complaints or concerns via physical mail. Information required for consumers to build a personalized identity theft recovery plan or electronically submit an Identity Theft Affidavit (Form 14039) to the IRS via IdentityTheft.gov is collected when a consumer fills out an identity theft report plan at www.IdentityTheft.gov. Consumer complaints relating to cross-border e-commerce fraud is gathered through www.econsumer.gov and provides online complaint forms in English, Spanish, French, German, Polish, Japanese, and Korean. Consumers who wish not to receive telemarketing calls can register their telephone numbers on the DNC, either online via the DNC website (www.donotcall.gov), or by calling the toll free phone numbers.

[13] See the FTC Surveys Privacy Impact Assessment for more information.

Source of Data	*Type of Data Provided & How It Is Collected*
CSN customer service representatives	Physical mail received by the FTC is scanned and sent to the CRC for processing. Authorized CSN customer service representatives then review and enter the data into CSN using the contact center complaint interface.
External data contributors	The major external data contributors to SNS currently include the following: Better Business Bureau (BBB), Consumer Financial Protection Bureau (CFPB), State Attorneys General (currently 21), Privacy Star, and Green Dot.[14] Most of the contributors send batched data using a secured Web interface. The FTC insists that all data sent by external organizations be encrypted and securely maintains the original data contributor files. For data files received via email or Web service, the FTC encrypts the data at rest.
Telemarketers	Telemarketer information gathered by DNC is provided by telemarketers and sellers through the telemarketer internet site (www.telemarketing.donotcall.gov).
External law enforcement partners	Law enforcement organization and user information for access to the CSN is provided directly by the law enforcement member and their respective organization. Law enforcement officials signing up for access provide information 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 mail, or fax.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
FTC employees and on-site contractors	Within the FTC, SNS data is used by attorneys, investigators, paralegals, data analysts, and economists to accomplish their consumer protection missions and 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. SNS data is also 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

[14] A complete list of data contributors is available in the FTC's annual Consumer Sentinel Network Data Book. SNS does not receive data from commercial data brokers or information resellers.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
	compiled from SNS data also help determine the effectiveness of the FTC's consumer protection program in accordance with the Government Performance & Results Act. All internal users have read-only access. 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 that they enter or update, and data contributors only can access parts of the system that will allow them to contribute their data. SSNs are not visible to FTC users or external law enforcement users. The FTC maintains audit logs of each user's activity in SNS to make sure that any data access can be traced for security reasons.
Leidos staff	The FTC's contractor involved with the design, development, and maintenance of the system, Leidos, has access to the SNS data to maintain and support the ongoing SNS operations including web portal hosting services and call center services. Leidos staff serve as Customer Service Representatives for the Consumer Response Center (CRC). For example, a call center Customer Service Representative interacts directly with consumers and records the data into the SNS system. Customer services representatives also have the ability to enter consumer complaint information in to the system and update consumer complaint records already entered, which they do when they received updated information from the consumer complainant.
Offsite Mailroom Digitization (BrightKey)	Physical mail received by the FTC is scanned by the agency's Offsite Mailing Digitization vendor (currently BrightKey). After the paper mail has been scanned, BrightKey sends the digitized mail to the CRC for processing. It is then reviewed and entered into CSN by customer service representatives using the contact center complaint interface. BrightKey staff do not have direct access to data in SNS. The digitized version of the mail is deleted from BrightKey's network within 48 hours. Hardcopy mail is retained for 20 business days before destruction. Within this 20 day timeframe, any hardcopy mail may be rescanned and emailed to the CRC, if necessary.
Telemarketers	Telephone numbers included in the DNC Registry are shared with telemarketers to ensure that telemarketers do not call those numbers. 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. Information provided by telemarketers to the DNC Registry is made available to both the FTC and CSN members for law enforcement purposes. Alleged DNC violations are publicized every weekday on the Do Not Call Reported Calls Data webpage.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
	This data contains the telephone number that made the unwanted call, when the call was made, the subject matter of the call, whether the call was reported as a robocall, and the complainant's city and state.
Federal agencies and external law enforcement partners	The FTC shares SNS data with other federal agencies and authorized law enforcement agencies.[15] If a user opts to submit an Identity Theft Affidavit (Form 14039) electronically to the IRS via IDT, the information provided to fill out the affidavit will be shared with the IRS. 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. 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. Consumer IP address information, collected to identify fraudulent, repetitive, or erroneous submissions, is also available to law enforcement agencies. However, IDT data is not available to all law enforcement agencies. 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 FTC Office of International Affairs (OIA) and the Office of General Counsel (OGC) are consulted on all decisions regarding sharing data with foreign entities. 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. The FBI Recovery Asset Team (RAT) will receive specific banking information regarding complaints within the ReportFraud portal in order to help victims of scams reverse high dollar, fraudulent banking transactions. When a case meets the criteria for FBI involvement, the complaint will be shared with the FBI RAT, and clearly set the expectation that the consumer could receive a contact, as well as how to validate that the contact is legitimate.

[15] For a complete list, see www.ftc.gov/enforcement/consumer-sentinel- network/members.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
Credit Reporting Agencies (CRAs) and consumer organizations	A limited number of employees at three national CRAs (Experian, Equifax, and TransUnion) have access to the Identity Theft Report Verification Portal, which verifies the validity of questionable identity theft reports. External users access the SNS applications through 256-bit TLS encryption and strong two-factor authentication. 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. When a consumer's IDT report appears to be potentially fraudulent, a limited number of CRA employees can use the Identity Theft Report Verification Portal to determine whether the first name, last name, and IDT report number match information contained in SNS.
Other external entities	The FTC may be required or authorized to share complaint data with external entities in other circumstances such as: responding to requests from Congress, Freedom of Information Act (FOIA) requests for FOIA-accessible information from the media (not obtained through a FOIA request)[16], or during the course of litigation or otherwise where consumer complaints may be disclosed to the subject of the complaint, to a court, etc. To the extent required or authorized by law, 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 FTC Office of the General Counsel and are granted only as permitted by law. 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.

[16] As part of the Commission's consumer education mission, the FTC provides aggregated data to the press to enable them to inform the public about consumer protection issues. The FTC does not disclose PII during this process.

3.2 Do contractors and/or third party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

FTC contractors with access to the data through collection and/or processing, as well as those tasked with technical support of SNS, submit to a rigorous security clearance process, sign a non-disclosure agreement, take annual privacy and security training, and agree to act in accordance with specified rules of behavior. Leidos 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. Leidos personnel receive refresher training annually. Customer Service Representatives also receive security awareness training on sensitive information and PII handling during orientation. The Leidos 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.

The FTC's mailroom vendor, BrightKey, has access to all physical mail sent to the FTC. Hardcopy mail is secured, screened, and opened by BrightKey employees at their offsite facility, then scanned and emailed to the intended FTC recipient. BrightKey is an approved and vetted contractor; only BrightKey employees authorized to handle FTC data can access and manage FTC mail. BrightKey staff do not have direct access to SNS.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third party service provider.

FTC contractors (including Leidos staff) who access SNS or have access to data intended for SNS (including BrightKey staff) are contractually bound to follow the rules and policies set by the FTC for privacy incident responses. Contractors must also follow the reporting and other procedures in the FTC's Breach Notification Response Plan.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

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. 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.

☒ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☒ Written ☒ Verbal)
- ☒ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☒ Login banner
- ☐ Other (*explain*):_____

☐ Notice is not provided (explain): _____

Additional notice is provided through the FTC's System of Records Notices (SORNs), which are published in the Federal Register, are posted and accessible online through the FTC's Privacy Act page, 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. The sites 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 to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

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. In IDT, consumers are informed that if they do not provide their phone number, city and state of residence, and email address – information necessary for an account – they will not be able to use the services provided to account holders. The data transmitted to the FTC by other entities is provided in accordance with those entities' policies and practices.
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.

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 also can choose to share their information with organizations that provide additional consumer counseling services. To do so, consumers must give express consent at the time they submit their complaint.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Consumers may request access to or correction of system records about them that are 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. Without filing such a request, consumers may update the information they provide in a complaint by calling the CRC at 1-877-FTC-HELP or 1-877-ID-THEFT. For identity theft complaints, consumers may log into their IDT account, using two-factor authentication, to access their complaint information and add, update, or remove their information as desired. 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 logging into the system and changing the information in their profile.

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

As specified above in Section 4.3, to the extent the Privacy Act applies, the FTC provides a process for individuals to correct or amend any inaccurate PII maintained by the FTC, including any information that may be stored in SNS. The FTC's Privacy Policy provides links to the FTC's SORNs, which include information about how to correct or amend records. An individual may make a request under the Privacy Act for access to information maintained by the FTC about themselves in Privacy Act systems, including data in SNS. Access to the information under the Privacy Act is subject to certain exemptions. Individuals may also file FOIA requests for agency records about them (if they are not exempt from disclosure to them under those laws). Additionally, individuals may contact the FTC with any complaints, questions or concerns via phone or email available on www.ftc.gov or contact the Chief Privacy Officer directly. Where appropriate, the FTC disseminates corrected or amended PII to other authorized users of that PII, such as external information sharing partners.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

Consumer complaints collected by the CRC, ReportFraud.ftc.gov, IDT and DNC, and complaints provided by data contributors are not checked by the FTC for accuracy or validity. This information is provided voluntarily by consumers and is made available for law enforcement use and investigation. 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 Leidos before the application is approved and the user is granted access.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

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 tokens, approved IP address ranges, and such other factors as the FTC may determine necessary to secure the system and its data. Similarly, consumers who wish to access their IDT account must use two-factor authentication. After logging in using a registered email address and password, a one-time passcode delivered to the consumers' telephones must be entered before the consumers gain access to IDT.

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.

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. When a complaint is filed by a child under the age of 13, any PII in that complaint is deleted and purged.[17] For DNC online registration, the online registration wizard only collects consumer telephone numbers and email addresses.

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

[17] 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.

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 the specific user to perform his/her specific function.
- Unsuccessful Login Attempts – System automatically locks the account when the maximum number of unsuccessful attempts are exceeded.
- Audit logs are reviewed for technical and administrative errors.
- Strong password requirement.

The customer service representative with whom the consumer chats and the automated Chatbot are trained or designed to provide information about technical assistance only and to avoid substantive advice or assistance that could lead to a consumer providing sensitive PII. If, during the course of the chat, a consumer submits sensitive PII in a recognizable format, such as SSN, bank account number or credit card number, that information is automatically redacted and stored only as Xs. Consumers cannot submit or complete an online complaint using the web chat or Chatbot function. The Chatbot will also notify the consumers that they will not be contacted as a result of the automated chat session. The entry to the web chat feature is located and accessed from the ReportFraud page, where there is also a link to the FTC privacy policy.

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.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process? .

☒ Not Applicable. PII is not used in the course of testing training, or research within the SNS system.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

SNS records are maintained in accordance with the NARA-approved record disposition schedule, DAA-0122-2021-0002, which was approved on May 17, 2022.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

Yes, the system uses Web sites or portals for information collection and access purposes. The tracking technology used by various Web components of the system (e.g., cookies) is described below.

For security and 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, ftccomplaintassistant.gov, and IdentityTheft.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. The IP address of the computer used by the consumer when submitting an Identity Theft complaint is collected to identify fraudulent, repetitive, or erroneous submissions.

SNS websites – including consumersentinel.gov, donotcall.gov, econsumer.gov, ReportFraud.ftc.gov, and IdentityTheft.gov – do not use persistent cookies or tracking mechanisms that collect PII. All of these websites do use session cookies, which are temporary files that are erased when a user closes her browser. Session cookies typically will store information in the form of a session identification that does not personally identify the user. 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 necessary to ensure the proper functioning of the websites. Users may not be able to use the SNS websites if they decline to accept session cookies. In addition, consumersentinel.gov and IdentityTheft.gov use authentication confirmation cookies, a type of session cookie that transfers the security and login information for the consumer from page to page. Because of the high level of security required to protect the information available in on these sites, these cookies are used to prevent members from having to re-authenticate themselves at each separate page. For more information, see the FTC's Use of Cookies.

SNS does not use persistent cookies, web beacons, Adobe flash cookies, or other persistent

tracking devices on the system websites. However, the SNS websites that employ Google Analytics do use persistent and temporary session cookies that collect information about the user's web browsing experience.[18] Microsoft Application Insights (MAI), also used by the FTC to provide analytics and support web performance, uses a multi-session tracker/cookie to provide telemetry data that measures website traffic, assess how visitors use the SNS websites, and distinguish unique users. Users are never tracked outside of boundaries of the SNS websites.

SNS uses 256-bit TLS encryption when personal information is collected through a website, page, or online form. Personal information that is collected from consumers, telemarketers and law enforcement agencies stored in the SNS database is also encrypted.

8 Privacy Risks and Evaluation

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

Risk	*Mitigation Strategy*
Inadvertent disclosure by external enforcement members	To mitigate the risk of disclosure 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. 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.
Consumers providing unnecessary PII	To mitigate the risk of consumers providing unnecessary PII, the CRC uses the online ReportFraud portal, 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. The FTC also trains the staff and customer service representatives working with consumers directly to collect only the information necessary to the specific complaint and not to collect unnecessary sensitive PII.

[18] See https://digital.gov/services/dap/common-questions-about- dap-faq/ for additional information about the cookies used by Google Analytics.

Risk	*Mitigation Strategy*
Unauthorized access to IDT	To mitigate the risk of unauthorized access to IDT, the IDT portal employs a secure two-factor authentication mechanism to ensure user authenticity. After logging in using a registered email address and password, users must enter a one-time code delivered to the user's telephone before the user gains access to IDT. This code is delivered via SMS or voice recording. The two-factor authentication process is enforced every time a user attempts to gain access to their IDT account. 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.
Inaccuracy of data provided by consumers and data contributors	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 accepts self-reported consumer complaint information and makes the process of filing complaints as easy as possible for consumers. CSN law enforcement members understand that they are accessing self-reported information that may not be accurate.
Collection of IP address and linking to user	The IP address information is typically collected for any website that maintains HTTPS access logs. SNS collects consumers' IP address information in order to protect the integrity and security of the consumer's web sessions, as well as to identify fraudulent, repetitive, or erroneous submissions. Any attempted misuse of such information is strictly prohibited. All user access and operations are logged, and logs are maintained on a centralized logging server. The logs are used to audit user access and produce relevant security reports.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

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 256-bit Transport Layer Security (TLS) 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 are encrypted at rest using software encryption. All encryption and data transport protocols meet OMB and NIST standards.

In accordance with OMB and NIST standards, access to the SNS CSN and Identity Theft

portals is strictly controlled and utilizes a minimum of two authentication factors. Authentication factors include: unique user names, passwords, one-time passcodes generated by 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 servers are protected through advanced firewalls and Intrusion Prevention Systems (IPS).

To increase efficiency and decrease costs, the SNS system is hosted in multiple secure cloud environments that provide services to federal and state government entities. These cloud environments have undergone an extensive Assessment and Authorization process conducted by a FedRAMP-certified third-party assessment organization.[19] SNS utilizes Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) from cloud service providers. In addition, SNS employs machine-learning technologies to analyze the data collected from various data sources.

SNS also employs a web chat service called Web Chat. This product allows customer service representatives, through encrypted connections, to help consumers filing an online complaint with their technical issues so that they can better navigate our complaint form. This service does not include any live screen shares or co-browsing, and consumers cannot use web chat to complete or submit a consumer complaint.[20]
In addition, SNS uses an automated 24x7 Chatbot service to assist consumers quickly connecting with the answers to frequently asked questions when they need to file a complaint.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

Yes. The Privacy Act SORN corresponding to general consumer complaint collection is currently designated FTC IV-1 (consumer complaints generally). Consumer complaint data can be retrieved by the following fields: consumer name, street address, telephone number, email address, and unique FTC reference number. Information about the entity or individual that is the subject of the consumer's complaint is retrieved by the following fields: organization name, street address, EIN or SSN, telephone number, first or last name, and email address. CSN member information is retrieved by: member first name or last name, and organization name. For complaints related to the accuracy of a consumer's credit report, SNS allows the consumer to provide an SSN. SNS encrypts the consumer's SSN, and the number is not displayed when users search the system. However, the system still allows users to search for complaints by specific SSNs.

In addition, the DNC is currently covered by the Privacy Act SORN currently designated as FTC- IV-3 (National Do Not Call Registry® System-FTC). Consumer complaint data is

[19] The FedRAMP website is available at www.fedramp.gov.
[20] Co-browsing, in the context of web browsing, is the joint navigation through the World Wide Web by two or more people accessing the same web pages at the same time.

retrieved by area code and phone number of individuals who have informed the Commission that they do not wish to receive telemarketing calls. This data may also be retrieved by other data, if any, compiled or otherwise maintained with the record. Telemarketer information is retrieved by the following fields: organization name, street address, EIN or SSN, telephone number, first or last name, and email address. Note: telemarketer business entities are not covered by the Privacy Act.

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),

The above SORNs are published in the Federal Register, and posted and accessible online through the FTC's Privacy Act page, www.ftc.gov/privacy. In compliance with the Privacy Act, the Consumer Sentinel website, which collects information from individuals subject to the Act, contains the required notice of authority, purpose, routine uses, and whether the collection is voluntary or mandatory. The system's various websites and portals also contain links to the FTC's Privacy Policy.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

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.