



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Consumer Information System

Privacy Impact Assessment

September 30, 2004

INTRODUCTION

The Federal Trade Commission's (FTC or the Commission) Bureau of Consumer Protection (BCP) protects consumers from fraud, deception, and unfair practices in the marketplace. The BCP addresses current issues of importance to consumers, including identity theft, telemarketing fraud, Internet fraud, and consumer credit. To further its consumer protection mission, the FTC files law enforcement actions and provides consumer and business education to protect the public. The FTC works to ensure that consumers have accurate information for purchasing decisions, and confidence in the traditional and electronic marketplaces.

The 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, and consumer and business education. The BCP uses the Consumer Information System (CIS) as the primary system to collect, analyze, extract, distribute, and archive/purge data relating to its mission. In addition to recording instances of business practices related to fraud, financial loss, identity theft, and Do Not Call regulations, CIS also facilitates consumer requests for educational material related to numerous business practices.

The BCP has conducted this Privacy Impact Assessment on the existing CIS as part of its Certification and Accreditation process for major information technology systems.

SYSTEM OVERVIEW

CIS in its current state evolved from past FTC systems, integrating the similar functionality of the older Consumer Complaint System (CCS) and the Telemarketing Complaint System (TCS). TCS incorporated several separate, older systems: Chairman's Correspondence Tracking System; Office of the Secretary Congressional Correspondence System; and other Commission correspondence tracking needs within the Bureau of Competition and the Office of the General Counsel. In 1992, CCS and the TCS sub-systems were merged into a single system, and redesigned in 1997 into a single CIS replacing all previous sub-systems, and configured to operate within the Oracle 6 RDBMS, Windows PC based Client Server Forms environment on a SUN UNIX server.

Expansions to CIS have included: the Correspondence Management System (1998); the Consumer Sentinel® Web site (1998); the Identity Theft (IDT) client-server application and the Web based IDT Data Clearinghouse (1999); toll free telephone numbers for consumers to report complaints (1999); "KnowFraud" Web link with the U.S. Postal Inspection Service (2000); a Web site for collection of cross-border e-commerce complaints (econsumer.gov) (2001); Consumer Planet Sentinel (2001); Military Sentinel (2002); and incorporation of Oracle portal (access control mechanism) (2002/3). In 2003, CIS was expanded to utilize a DataMart, which is the repository of CIS data that provides query and reporting functions for the Consumer Sentinel Network (described below). In addition, Business Objects reporting software is utilized for in-depth analysis of CIS data.

As a central repository for complaint data, CIS is a powerful crime-fighting data source, much of which is available to the federal, state, and local, as well as the international, law enforcement community. CIS data are also used to identify and track trends and potential problems affecting the marketplace.

CIS contains data collected by the FTC as well as data collected by other entities that are forwarded to the FTC. External contributors include a broad array of public and private domestic and foreign organizations.

Other applications or components of CIS that are used to collect or share consumer data are:

- **Consumer.gov public Web sites**, where consumers can lodge complaints, obtain educational materials, and view trends in fraud and identity theft. These sites also provide information to law enforcers and businesses. Complaints are entered into CIS.
- **Consumer Sentinel[®] Network (CSN)** is a series of interconnected Web-based applications, or portals, through which authorized external law enforcement users can access various subsets of complaint records in CIS. These applications include: Consumer Sentinel[®], the Identity Theft Data Clearinghouse, Consumer Planet Sentinel, and Military Sentinel. External users have access only to CSN, and not directly into CIS. (Only FTC staffers and contractors have direct access to CIS.)

The purpose of CSN is to share information about consumer fraud (including Do Not Call) and identity theft with law enforcers for law enforcement purposes. As of September 1, 2004, CSN served about 1,200 law enforcement agencies across the world that have signed appropriate confidentiality agreements restricting their use and disclosure of CIS data to law enforcement purposes. Authorized users access CSN through a secure, password-protected Web site. They then can search a subset of the complaints in CIS (as described below). (CSN users' access to the various subsets of CIS data is based on the organization to which they belong.) Search criteria includes, among other things, company or suspect name, address, telephone number, consumer location, or type of scam or identity theft.

- **Consumer Sentinel[®] (CS)** is the application through which local, state and federal law enforcers in the United States, Canada and Australia access consumer fraud, identity theft and Do Not Call complaints. CS users have access to all consumer fraud and DNC complaints. Only domestic and Canadian law enforcers have access to identity theft complaints, per the restrictions stated in the next paragraph.
- **The Identity Theft Data Clearinghouse** is the nation's repository of identity theft complaints. These complaints are entered into CIS. Users access the Clearinghouse through CSN. Currently, all US law enforcers can access complaints in the IDT Data

Clearinghouse. Canadian law enforcers can access all IDT complaints submitted by Canadian data contributors as well as IDT complaints submitted by US data contributors that have an entry date after July 1, 2003.

- **Consumer Planet Sentinel (CPS)** 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. CPS is part of econsumer.gov (www.econsumer.gov), an international project focusing on cross-border e-commerce fraud. The econsumer.gov site offers cross-border consumer protection information and an online complaint form. All information on econsumer.gov, including the complaint form, is available in English, Spanish, French, German and Korean (currently, there is no Korean language complaint form). Cross-border e-commerce complaints received from consumers through the econsumer.gov complaint form are entered into CIS. CPS users can access only those complaints received through econsumer.gov.
- **Military Sentinel**, launched in September 2002, 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 (MS) consists of a public Web site, and a restricted Web site accessed through CSN. The MS public site also provides a gateway to consumer education materials covering a wide range of consumer protection issues. Information from complaints entered through MS helps target law enforcement actions and consumer education initiatives.

The complaint forms on the MS public site allow consumers to identify their service branch, posting and pay grade. Consumer fraud and identity theft complaints entered into MS go directly into CIS, and are accessible by users through CSN. Also, consumer complaints submitted through MS's public Web site are accessible by DOD consumer education staffers through the MS restricted Web site, although consumers' personal identifying information (e.g., name, address, telephone number) is not displayed.

- **The National Do Not Call Registry (DNC)** was created by the FTC through amendments to its Telemarketing Sales Rule. The registry is a central database of telephone numbers of consumers who choose not to receive telemarketing calls as well as profile information about the organizations that have registered to download these phone numbers. The registry also lists the area codes that were purchased and downloaded by those organizations. Consumers are able to register either online or by telephone. The rule currently requires that telemarketers search the registry every three months and delete (or "scrub") from their call lists phone numbers that are on the registry (as of January 2005, telemarketers will be required to scrub their call lists every 31 days). Consumers who receive telemarketing calls after they have registered their telephone numbers may lodge complaints either online or by telephone.

The FTC has contracted with AT&T Government Solutions, Inc. to implement and maintain the consumer and telemarketer registries, and to receive consumer complaints. AT&T transmits all consumer complaint information received to the FTC for storage in

CIS on a daily basis. Registry information on consumer telephone numbers and organizations is available through queries from within Consumer Sentinel®.

ANALYSIS

1. The Information CIS Collects from Consumers

CIS collects and maintains personal information that consumers voluntarily submit either when they contact the FTC or another entity that contributes data to CIS. This personal information includes: first and last name; street address; city; state; zip code; email address; date of birth or age range; and telephone number(s). For two categories of complaints – identity theft-related complaints and complaints related to the accuracy of the consumer’s credit report – CIS permits consumers to provide a Social Security number.¹ CIS encrypts the Social Security number, and the number is not displayed when users search the system. CIS also collects and maintains the subject matter of consumers’ complaints (a 2,000 character free text “comments” field) and information regarding the companies, entities, or individuals about which the consumer is complaining.

The FTC collects such information directly from consumers, who may provide it by using the FTC’s online consumer complaint forms, or by calling, writing or visiting the FTC’s Consumer Response Center at 600 Pennsylvania Avenue NW, Washington, D.C. The FTC also collects consumer complaint data from external data contributors that share consumer protection-related complaints with the FTC. Each of these methods of collection is discussed below.

a) Collection from consumers through the FTC’s online complaint forms: The FTC operates several public Web sites where consumers can lodge general consumer and identity theft complaints, obtain educational materials, and view trends in fraud and identity theft. Consumers also can access an online complaint form directly from the FTC’s primary Web site at www.ftc.gov. General consumer and identity theft complaint forms are available in English and Spanish. The other public Web sites through which the FTC collects online complaints that are entered into CIS are:

- The Consumer Sentinel® public Web site (www.consumer.gov/sentinel) for consumer complaints;
- The IDT Web site (www.consumer.gov/idtheft) for identity theft complaints;
- The Do Not Call Web site (www.donotcall.gov) for complaints related to

¹ See Fair Credit Reporting Act Complaint Referral Program Privacy Impact Assessment (September, 2004).

violations of the Telemarketing Sales Rule and the Do Not Call (DNC) Registry;

- The econsumer.gov Web site (www.econsumer.gov) for complaints relating to cross-border e-commerce fraud (which provides online complaint forms in English, Spanish, French, and German); and
- The Military Sentinel public Web site (www.consumer.gov/military), for complaints from service members, their families, and DOD civilians. In addition to the standard information collected on the FTC's other online complaint forms, the complaint forms on Military Sentinel allow consumers to identify their service branch, posting and pay grade.

b) Consumer Response Center: Consumers also may lodge complaints directly with the FTC by calling one of several toll free telephone lines, sending a complaint in writing, or visiting the FTC at 600 Pennsylvania Avenue NW, Washington, D.C. These complaints are handled by the FTC's Consumer Response Center (CRC). The CRC, which includes FTC employees and contractors who are bound to maintaining the confidentiality of the information by a non-disclosure agreement, receive, process and input complaints into CIS.

c) External data contributors: CIS includes data collected by other entities that are forwarded to the FTC. External contributors include a broad array of public and private domestic and foreign organizations. Most of those contributors send batched complaint data using CD's or email.²

d) National Do Not Call Registry: Consumers may register for the National Do Not Call Registry either by phone or online at www.donotcall.gov. Consumers must provide the telephone number(s) they are registering and, if they register online, an email address (the email address is encrypted).

2. Why the Information Is Being Collected

The FTC collects and maintains consumer complaints to further its consumer protection mission. By collecting, maintaining, and analyzing CIS data, the FTC is better able to identify trends in consumer fraud and law violations, target law enforcement action, and provide consumer and business education to protect the public.

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

² For a list of external data contributors, see www.consumer.gov/sentinel.

concerning and to investigate business practices in or affecting commerce, with certain exceptions. The Identity Theft and Assumption Deterrence Act of 1998, 18 U.S.C. § 1028 note, mandates the Commission's collection of IDT complaints. In addition, 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 DNC-related complaints. These collections have been reviewed and approved by OMB (OMB Control No. 3084-0047) in accordance with the Paperwork Reduction Act.

3. The Opportunities Consumers Will Have to Decline to Provide Information or to Consent to Particular Uses of the Information

All information provided by consumers to the FTC is voluntary. Consumers may choose to submit some, all, or none of the personal identifying information requested by the FTC's complaint forms. Through notices available on the online complaint forms and provided by telephone counselors, 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.

4. How Information Collected From Consumers Is Used And Disclosed

The FTC uses and shares CIS data to further its consumer protection mission. The use of CIS data is in accordance with the routine uses outlined in the FTC's Privacy Policy and Privacy Act System of Records notices.³

- a) **FTC Staff and Contractors:** CIS data are used by FTC employees and contractors to target investigations, locate fraud victims, respond to inquiries, provide consumer and business education, and identify trends. In addition, CIS data are 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 of CIS data also help determine the effectiveness of the FTC's consumer protection mission (e.g., Government Performance & Results Act).

Within the FTC, CIS data are used by BCP and regional office consumer counselors, attorneys, investigators, paralegals and data analysts; the Office of the

³ For FTC Privacy Policy, see <http://www.ftc.gov/ftc/privacy.htm>. For Privacy Act System of Records notices, see 57 FR 45678 (Oct. 2, 1992) (consumer complaint system generally), 64 FR 57887 (Oct. 27, 1999) (IDT portion), and 68 FR 37494 (June 24, 2003) (National Do Not Call Registry).

General Counsel; the Office of the Secretary; the Bureau of Economics; and the Office of the Inspector General.

- b) **External law enforcement:** As part of its consumer protection mission, the FTC shares CIS data with other law enforcement agencies. Through CSN, various subsets of CIS data are shared with authorized local, state, federal, and international law enforcement officers.

Periodically, the FTC provides law enforcement agencies with batched data using a CD. This information is password protected, and encryption used in CIS is maintained in the data transfer.

- c) **Other disclosures:** The FTC may be required or authorized to share complaint data 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. In these situations, the FTC redacts all personal identifying information before providing the CIS data. Governmental agencies also may request CIS data for a non-law enforcement purpose (e.g., regulatory entities may use for licensing) (such requests must be submitted to and approved by the Office of the General Counsel). CIS 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 CIS data after receiving assurances of confidentiality from the recipients.
- d) **FCRA Complaint Referral Program:** The FTC may share certain consumer complaints about identity theft or the accuracy of a consumer's credit report with credit bureaus to help address the consumer's complaint or identity-theft related concern. The credit bureaus will review the complaints, take appropriate action, and report back to the Commission on their determinations. In addition, the repositories will share some of the complaints with consumer reporting agencies that maintain consumer files within the systems operated by the repositories ("associated consumer reporting agencies" or "associated CRAs"). The repositories 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.⁴

5. Security

⁴ See Fair Credit Reporting Act Complaint Referral Program Privacy Impact Assessment (September, 2004).

CIS employs multiple security controls to protect the privacy related information it collects. Verisign digital certificates provide Secure Socket Layer (SSL) communications and authentication for external users of CSN. Social Security numbers are encrypted in CIS. Access control mechanisms restrict users to authorized actions or tasks based on appropriate privileges (i.e., external law enforcers cannot change data within CIS; CRC staffers can update data in case a consumer provides additional or changed information). Another feature of the system is the inability to access any data outside of the application front end. Users cannot use SQL-Plus or other tools to access that data even if they log on with a user ID that is in the access list. External access to CSN is protected by a firewall.

Further, the Commission:

(I) Affirms that it followed IT security requirements and procedures as required by federal law and policy to ensure that information is appropriately secured;

(II) Conducted a Risk Assessment, identified appropriate security controls, and implemented those controls;

(III) Conducted all security related activities required by the Commission's Certification and Accreditation Policy including, conducting a risk assessment to identify appropriate security controls, development of a system security plan to document the managerial, technical and operational controls used by the system, and conducted security testing and evaluation of the system by an independent party to verify that the specified controls were in place and operating as expected. The system will be scanned monthly to ensure that implemented controls continue to operate as expected and to identify and mitigate any new vulnerabilities. The system will be subjected to a 'self-assessment' evaluation of risk on an annual basis and a new risk assessment and system security plan will be developed every three years or when there are significant changes to the architecture of the system;

(IV) Designates the Office of Information Technology, Office of the Executive Director, Federal Trade Commission, as the point of contact for questions about the technical controls on this system.

6. Privacy Act

CIS is covered by three existing Privacy Act System of Records notices, available at 57 FR 45678 (Oct. 2, 1992) (consumer complaint system generally), 64 FR 57887 (Oct. 27, 1999) (IDT portion), and 68 FR 37494 (June 24, 2003) (National Do Not Call Registry). In compliance with the Act, the Web sites from which consumers can access the general, IDT and DNC 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.

7. Other Privacy Considerations And Analysis

The FTC has identified privacy risks associated with CIS and has taken steps to mitigate those risks. With respect to the collection of data, the risks we identified are: consumers might not understand how their information will be used, children under the age of 13 may attempt to provide us with personal identifying information, consumers might not realize the protection that is accorded their information, and we might collect more information than is required (e.g., consumers provide Social Security numbers on the general complaint form when not needed). To address these risks, we provide clear and conspicuous notice (on our online complaint forms or through a telephone counselor) about how consumers' information will be used. On the online complaint forms, we provide a link to our Privacy Policy. Social Security numbers, if provided, are encrypted when stored in CIS. We explain on our general complaint form that a Social Security number should be provided only for certain types of complaints, and CIS is designed to not store the Social Security number if provided inadvertently for a different type of complaint. Our Web sites are not directed to children under 13, and if an individual lodges a complaint and indicates that he/she is under 13, we delete/purge any personal identifying information in that complaint. We do not use persistent cookies or other tracking devices on our Web sites. We use SSL encryption to protect data transmitted using our online complaint forms.

With respect to the use and disclosure of CIS data, the FTC recognizes that there is a risk that consumers' information will be misused or disclosed for an unauthorized purpose. To mitigate this risk, the FTC has taken a number of steps. First, we require all of our contractors involved with data collection and processing, as well technical support of CIS, to pass a security clearance. Second, all contractors are required to sign a non-disclosure agreement.

Further, we limit users' access to data and functions based on their role. Each user is assigned a unique user name and password (passwords must be strong - i.e., at least 8 characters; contain a mix of letters, numbers and special characters; and not be based on a word in any language, slang or jargon). Access to CIS is password protected. Access to CSN requires dual verification - a digital certificate and a password. In addition, by using a portal mechanism, users are limited in the functions they can use and have access only to specific subsets of the data. For example, the contractors involved with data collection can only view the data which they enter, and CPS users only can view data received through econsumer.gov. Users cannot see Social Security numbers. External users enter CSN through SSL. We also can maintain audit logs of each user's activity in CIS.

In addition, we protect use of the information by external law enforcers through a confidentiality agreement. Each member agency, and each user, agree, in writing, to maintain the confidentiality of CIS data and only to use it for law enforcement purposes. In addition to the confidentiality agreement, we periodically provide CIS users with information on how CIS data may be used and disclosed. If we disclose CIS data in another manner (e.g., in response to a FOIA request or to an entity that is a subject of a complaint), we redact personal identifying information.

As for storage of the information, there is a risk that unauthorized users may try to access

CIS. This risk is addressed in the Security section above. The Commission may retain data in CIS indefinitely, subject to earlier deletion.

Prepared for the Business Owner of the System, the Bureau of Consumer Protection, by

Jay M. Miller, Consumer Sentinel Program Manager, Division of Planning and Information, Bureau of Consumer Protection

Review:

Alexander C. Tang, Attorney
Office of the General Counsel

Privacy Steering Committee
By: Judith Bailey, Chair

Approved:

Stephen Warren
Chief Information Officer
Federal Trade Commission