Federal Trade Commission
Privacy Impact Assessment

for the:

Gilardi & Co., LLC Claims Management System and Online Claim Submission Website

January 2015

1 System Overview

The Federal Trade Commission's (FTC) Bureau of Consumer Protection (BCP) brings law enforcement actions that can result in the recovery of redress money from defendants that is to be returned to consumers or businesses from whom it was taken. Disbursement of money in the redress fund is made pursuant to a distribution plan that is either approved by a court or an administrative law judge or delegated to the FTC's discretion. The FTC's Redress Administration Office (RAO) is responsible for administering and coordinating redress activities, and Gilardi & Co., LLC ("Gilardi"), an FTC claims administration contractor, supports RAO's activities. This Privacy Impact Assessment (PIA) explains what Personally Identifiable Information (PII) RAO and Gilardi collect throughout the redress administration process, who is allowed to use this information and for what purposes, and what steps are taken to identify, secure, and reduce any privacy risks to that information.

Gilardi's claims management system stores consumer and business data, provided by RAO or obtained directly from individuals who submit redress claims, in a proprietary database.

Gilardi's system also has a public interface that permits individuals and businesses to complete and submit an electronic claim form via a website. Gilardi uses the data from the system to fulfill its role as the redress claims administrator, which includes the following duties: (i) to intake and process claims filed; (ii) to answer questions from FTC and other authorized parties; (iii) to answer questions from claimants and potential claimants as to eligibility and status of materials filed; (iv) to route claims to the claims administrator; and (v) to issue and track payments to authorized claimants.

Gilardi maintains physical systems in their secure on-site location in San Rafael, California.

2 Information Collected and Stored within the System

2.1 What information is to be collected, used, disseminated, or maintained by the system?

The claimant information that is collected, used, disseminated, or maintained either within RAO or within Gilardi's claims management proprietary database varies depending upon the redress matter. In routine redress matters, the following information is used: first and last name, business name (if needed), unique claimant ID, street address, city, state, postal code, country, home phone number, work phone number, email address, transaction data, transaction dates, product type, company selling product, customer number, customer account number, loss amount, and notes of claimant contact with Gilardi, including any subsequent change requests, updates, corrections, etc. In rare instances, Social Security numbers (SSNs), Tax ID numbers, credit card numbers, bank account numbers, and/or bank names may also be collected and used, only when no other key identifier is available.

In some cases, a consumer may call Gilardi regarding a redress matter. When applicable, the Gilardi Interactive Voice Response and Contact Center systems record the number that the individual calls from, the date/time/length of call, and the contact center script and skillset used

to route the call. Details of calls may be summarized in the Gilardi claims management system by claims processing staff.

2.2 What are the sources of the information in the system?

Claimant information comes from three primary sources:

- initial source data found in defendants' files and in consumer complaints submitted to the FTC and transferred to Gilardi;
- mailing address updates and corrections provided by third-party data sources such as the United States Postal Service (USPS) and address-tracing companies; and
- data provided directly by claimants as part of the redress administration process.

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

Claimant information is collected, used, disseminated, or maintained by RAO staff and Gilardi to identify potential claimants, to validate claimants and their claims, and to distribute redress payments to appropriate claimants.

2.4 How is the information collected?

The FTC collects consumer information directly from defendants' files when available. The FTC also collects consumer information from complaints that have been submitted directly to the FTC or to another organization that shares its consumer complaints with the FTC. The FTC claims administration contractor may collect supplemental information, in the form of address updates and corrections, from third-party sources. Consumer information is also collected directly from potential claimants via completed claim forms, correspondence with the FTC and/or Gilardi, via telephone calls, and using secure websites.

2.5 How will the information be checked for accuracy and timeliness (currency)?

Various steps are taken to validate the accuracy and timeliness of collected data based on its original source. For example, prior to the contractor mailing a claim form, redress check, or consumer education material, claimant addresses are standardized and cross-checked against known data sources, such as the USPS National Change of Address Database and U.S. Postal Service records regarding street names and address ranges. All resulting additions, deletions, and address changes to the data set are approved by the RAO and reconciled against the original source data.

In many instances, claimant data obtained from defendants' files can be used to mail redress checks directly to injured consumers and businesses. In other cases, individuals are contacted to provide or verify their information themselves. For example, claim forms may be mailed to a known set of claimants requesting that they validate, under penalty of perjury, their address, loss amount, and entitlement to redress. In other cases, claim forms will be made available to previously unknown claimants via case-specific redress notification and outreach. Again, claimants provide claim information, including their address, injury amount, and entitlement to redress, under penalty of perjury.

The redress contractor reviews claimant names, check distributions, and claim form responses to confirm that the loss amounts claimed are consistent with the established case-

specific claim parameters. Outreach material, redress checks, and claim forms always include an FTC website address for additional information, and a telephone number and mailing address for consumers to contact the redress contractor to have their questions answered and/or to update their information.

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

No.

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

The FTC collects this information in order to provide redress to injured consumers as part of its law enforcement activities pursuant to the FTC Act, 15 U.S.C. §§ 41-58, and other applicable statutes.

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

In the vast majority of redress matters, the information stored by RAO and Gilardi is limited to name, contact information, and claim information, possibly coupled with validation under penalty of perjury, in order to minimize privacy risks.

As discussed later in this document, comprehensive data security plans have been implemented to protect all data, including frequent, automated scans of information systems as well as policies and procedures to limit access to sensitive data and to ensure compliance with federal data privacy standards.

3 Use and Access to Data in the System

3.1 Describe how information in the system will or may be used.

Gilardi's system will be used to maintain claimant information for verification and record-keeping purposes relating to redress in FTC matters, and also to calculate and distribute redress payments. These activities may include printing and mailing claim forms, processing claims and corrections submitted by claimants, issuing checks or other forms of payment, and providing consumer education.

Prior to maintaining and disseminating claimant data, RAO staff removes all unnecessary information from the claimant data file, and RAO staff only forwards encrypted data to redress contractors. Similarly, Gilardi is instructed to collect the least amount of claimant information necessary.

Data in the system will be accessed only by authorized RAO and Gilardi staff to review and determine claimant eligibility for redress. The data will be accessed via secure login, and access will only be made available to authorized staff on a need-to-know basis. Data usage is in accordance with the uses described in the contract Gilardi has with RAO to support RAO's activities.

Data collected by Gilardi in a specific FTC matter may also be used by the FTC and Gilardi to identify potentially fraudulent claims submitted in other FTC redress matters. For each redress matter managed by Gilardi on behalf of the FTC, Gilardi sends a complete list of claims filed to the FTC. In an effort to identify potentially fraudulent claims, the FTC may analyze that information, refer back to data received in all redress matters past and present, and provide information regarding potentially fraudulent claims back to Gilardi.

3.2 Which internal entities will have access to the information?

Authorized RAO staff have access to the information, as do authorized Gilardi staff within the following functions:

- Information Technology professionals, for the purpose of importing, validating, updating, and storing claimant data;
- Claims processors, for the purpose of validating eligibility, communicating with claimants, and updating their contact information; and
- Management, for the purpose of reporting, supervising technology and processor resources, and ensuring accuracy and adherence to data handling standards.

RAO staff and Gilardi managers and supervisors of Gilardi staff who have access to claimant information have completed FTC-approved background checks and clearance. In addition, all Gilardi employees who have access to claimant information receive background checks conducted by Gilardi.

3.3 Which external entities will have access to the information?

No external entities other than claimants will have direct access to claimant information. Individual claimants may submit information directly, but once submitted, claimants can only view, not change, their information. The FTC may share claimant information occasionally with law enforcement and other government agencies, courts, and defendants, or as otherwise authorized by the law. RAO and Gilardi will securely download and transmit required data in response to authorized requests.

4 Notice and Access for Individuals

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

Individuals receive notice about the FTC's collection, use, and disclosure of their information through the FTC's Privacy Policy, at http://www.ftc.gov/site-information/privacy-policy.

In addition, redress cases that require Gilardi to collect claimant information via a claim form will always provide claimants with a Privacy Act statement, whether the claim form is paper or Web-based. The Privacy Act statement explains the authority, purpose, and routine uses of the information to be collected, whether the information is voluntary or mandatory, and any consequences if the information is not collected (e.g., the FTC may be unable to pay the individual his or her redress claim).

Claimants who submit consumer complaints to the FTC via the FTC online complaint form or FTC telephone complaint system receive a similar Privacy Act statement at the time they submit their complaint, and their relevant consumer complaint information is then forwarded to Gilardi for processing. Such notice is not provided to claimants if the FTC gathered their information solely from defendant's files, but such claimants may learn about the FTC's collection, use, and disclosure of their information through the FTC's privacy policy, as noted above. All claimants who receive a Privacy Act statement are also provided a mailing address and telephone number to update and provide additional information about themselves and their status.

As previously mentioned in section 2.5, all redress checks also include a mailing address and/or telephone number to allow consumers to contact Gilardi concerning their information. In instances where consumers can call the telephone number dedicated to the redress matter, the initial greeting and menu provides them with an option to listen to a Privacy Act statement.

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

Yes. The right to participate is voluntary, as explained in the Privacy Act statement. However, failure to submit the necessary information to authenticate the claimant and validate the claim may delay processing or result in rejection of the claim.

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

No. Consumers who choose to submit a claim do not have the right to limit their consent to particular uses of their information. They consent to their information being used as described in the Privacy Act statement. The consumer exercises this consent by choosing to complete, sign, and submit a claim form.

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

Claimants can access and view the status of their claim using a Gilardi web portal, but they cannot access, view, or edit their completed claim record. Instead, Gilardi initially enters the claimant data verbatim from hard copy and online forms submitted by the claimants or

creates a claim record from information submitted to them by the RAO. If a claimant's information is incomplete, Gilardi sends a letter informing the claimant that their claim is incomplete and explaining what is missing, and the claimant is sent a new, blank copy of the claim form to be used to complete the information.

Claimants can access their claim record by contacting Gilardi. Before making requested changes to a claimant's information, Gilardi will confirm the claimant's identity by asking a series of questions, including the tracking number, mailing address on file, SSN (if one has been collected for the limited purposes described in sections 2.1 and 2.8), and password, and instructing the claimant to forward their change request in writing along with supporting documentation if needed. Gilardi accepts written documentation via fax, mail, or email. The system does not display/send PII as part of the inquiry process. If PII is collected and/or transmitted, encryption methods are implemented to project sensitive information. Finally, claimants can obtain access to their own information through a Privacy Act request filed with the FTC's FOIA office. See the FTC's FOIA page at www.ftc.gov for more information.

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

The risk associated with allowing individuals to access their information online through the Gilardi-operated Web site is mitigated by the fact that individuals have read-only access to their claim in a specific matter, and they can view only their own information. The risk of unauthorized access to a claimant's claim is mitigated by security controls, including username and password authentication, application-layer security, unique claim identifiers, system-generated passwords, and password encryption.

Alternatively, if an individual seeks access to their information through the FTC's FOIA office, the risk of unauthorized disclosure is mitigated by procedures for asking the individual to verify his or her identity in writing, or, if the individual has authorized a representative to have access, to provide proof of such authorization in writing. See the FTC's FOIA page at www.ftc.gov for more information.

5 Web Site Privacy Issues

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

Gilardi does not host any permanent websites on behalf of the FTC. However, Gilardi may host a temporary website in a particular redress matter when the FTC determines it is appropriate and necessary to support online electronic claim submission. Persistent tracking technologies will not be used on these temporary, matter-specific redress sites. Temporary session cookies will be used for user session verification and will be terminated at the end of the visit. These cookies do not hold any PII, and the information they obtain cannot be directly correlated to an individual claimant. Gilardi staff reviews each temporary website for compliance with federal privacy requirements. In accordance with Federal guidance, including

Office of Management and Budget (OMB) Memorandum M-10-23, the FTC provides exit scripts to website visitors who click on links that will take them from FTC.gov and other official FTC resources to a website hosted by Gilardi.

In compliance with the Privacy Act of 1974, the E-Government Act of 2002, guidance issued by OMB, and the FTC's own Privacy Policy, the FTC mandates that Gilardi limit the collection of information from website visitors to the information necessary to assess and improve user experience, respond to consumer concerns, and administer redress.

To the extent that Gilardi's web hosting provider collects standard web log data, such as IP address, date and time of visit, and other required information, for cyber security and management reporting, such collection is in compliance with the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541, et seq.

5.2 If a persistent tracking technology is used, ensure that the proper issues are addressed (issues outlined in the FTC's PIA guide).

Not applicable.

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

Yes. The 256-bit SSL encryption algorithm is used to protect all external communications.

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

See Section 4 above.

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

In considering the Gilardi system, the following privacy risks were identified:

- When submitting a claim form, a claimant might inadvertently provide PII, including sensitive PII or health information, that is not required or requested for claims processing or verification;
- Data provided by individuals might not be accurate, complete, or timely; and
- Data provided by claimants might be misused or improperly disclosed or accessed.

To mitigate the risk of unnecessary PII being provided by claimants, the claim forms do not include an open-text comments field. Furthermore, fields are limited to the minimum information necessary to process a claim to reduce the risks of a user accidentally providing unnecessary information. SSNs are not routinely collected on claim forms.

As to the risk that the data provided might not be accurate, complete, or timely, it is important to note that individuals voluntarily provide claim information on the website, so that they may receive redress. The process of filing claims is made as easy as possible for individuals. Claimants have the ability to validate and verify claimant information and to update any inaccurate information, as described in section 4.4.

To mitigate the risk of the use and disclosure of consumer data, Gilardi employs a significant number of layered technical controls to help prevent the misuse or improper disclosure or access to consumer data. These controls include, but are not limited to the following:

- The Gilardi websites are hosted within a FISMA-accredited boundary;
- The Gilardi websites are maintained on a separate network segment from the consumers' specific claims data;
- Username and password authentication is negotiated via application layer security;
- Claimants are provided a unique claim identifier and a system-generated password;
- Passwords are encrypted when transmitting between the web server and client based computing device;
- Administrative controls include a number of failed attempts and lockout, server event logging, and IP address temporary tracking.

The Gilardi claims management system uses a defense-in-depth strategy to protect system resources against attacks by utilizing security technologies and services that maintain the Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation requirements outlined in National Institute of Standards and Technology (NIST) Special Publication 800-53.

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

Not applicable.

6 Security of Information in the System

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

Yes. Gilardi employs both information security and physical security for the information it collects. Gilardi is categorized as moderate system using Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems. The claims administration contractor has received an Authorization to Operate (ATO) from the FTC. The ATO was issued in accordance with FISMA following guidance provided by NIST. Contractor systems are routinely reviewed by the FTC to ensure compliance with FISMA.

6.2 Has a Certification & Accreditation been completed for the system or systems supporting the program?

Yes.

6.3 Has a risk assessment been conducted on the system?

Yes.

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

No. The technology employed to support FTC RAO does not raise any privacy concerns not already addressed. World Wide Web (HTTPS) technology is used within a closed network that is not accessible outside of their facility. To ensure the privacy of the data, the system uses Secure Socket Layer (SSL) encryption between the server and each user. Each user must use a secure password to gain access to the system as a whole, and then only users authorized to work on a particular redress matter have access to that matter's data.

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

Gilardi has account management policies and controls in place to manage its claims management system accounts, to include the establishment, activation, modification, and termination of system accounts. Gilardi account management activities include:

- Identification of account types;
- Conditions for group membership;
- Identification of authorized users specifying access privileges;
- Requirement of appropriate approvals for requests to establish accounts;
- Establishing, activating, modifying, disabling, and removing accounts;
- Specifically authorizing and monitoring use of the guest/anonymous and temporary accounts;
- Notifying account managers when temporary accounts are no longer required and when users are terminated, transferred, or access requirements change;
- Deactivating temporary accounts and accounts of terminated users as required;
- Granting access to the system based on valid access authorization, intended system usage, and other attributes as required by the organization;
- Reviewing accounts quarterly, at a minimum.

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

Gilardi employs formal, documented procedures to facilitate security awareness training, including a specific course related to PII, which is managed and implemented by Gilardi's Security Team and Human Resources. Additionally, all users involved with this and other FISMA-moderate client data are required to read and acknowledge all relevant policies and control standards.

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

Audit trails maintain a record of authorized and unauthorized system events both by system and application processes and by user activity of systems and applications. Audit logging is continuous, and logs are archived to provide access for review. In conjunction with other processes and controls, such as incident response capabilities and user identification and authentication, audit trails can assist in detecting security violations, network performance problems, and flaws in applications. Audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis. The Gilardi system is periodically reviewed by FTC staff as well.

6.8 Questions regarding the security of the system.

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

7 Data Retention

7.1 For what period of time will data collected by this system be maintained?

All records and documentation will be maintained for the duration of the claim process plus a minimum of three additional years after the claim process is completed.

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

At the end of the required retention period, Gilardi shall transfer a trustworthy electronic copy of the records and documentation to RAO. After review and approval of RAO, Gilardi shall then destroy all records and documentation in its possession associated with the matter, in accordance with NARA, OMB and NIST regulations and guidelines.

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

All data is stored within Gilardi's secure, layered environment and is encrypted to mitigate risks. Full backups of all production data are routinely conducted. Encrypted backups are replicated to an off-site datacenter through a dedicated, secure connection, for business

continuity purposes. Gilardi will dispose of the data in accordance with NARA, OMB, and NIST regulations and guidelines.

8 Privacy Act

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

Yes. Consumers are assigned a unique ID for identification, tracking, and reporting purposes. The following Gilardi roles have access to this data information using the unique IDs:

- Data Entry/Production
- Client Services/Call Center
- Data Analysis
- Case Management
- Claims Analysis

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

Yes. The redress contractor databases are covered by existing Privacy Act System of Records Notices, for nonpublic FTC program records, FTC-I-1, and for computer system user and identification and access records, FTC-VII-3, both of which can be viewed online at http://www.ftc.gov/about-ftc/foia/foia-reading-rooms/privacy-act-systems.

9 Privacy Policy

9.1 Confirm that the collection, use, and disclosure of the information in this system have been reviewed to ensure consistency with the FTC's privacy policy.

The collection, use, and disclosure of information from the Gilardi claims administration system has been reviewed to ensure consistency with the FTC's Privacy Policy.

Approval and Signature Page

Prepared for the Business Owners of the System by:

_____ Date: _____
Gregory W. Fortsch
Assistant Director, Division of Planning and Information

Concur:

_____ Date: _____
Gilardi & Co., LLC
Kim A. Wagner
Executive Vice President, Operations

Review:

_____ Date: _____
Alexander C. Tang, Attorney
Office of the General Counsel

_____ Date: _____
Peter B. Miller
Chief Privacy Officer

_____ Date: _____
Jeffrey Smith
Chief Information Security Officer

_____ Date:_____
Jeff Nakrin
Director, Records and Filings Office

Approved:

_____ Date:_____
Bajinder Paul
Chief Information Officer