U.S. Securities and Exchange Commission

Financial Investigative Software (FIS)
PRIVACY IMPACT ASSESSMENT (PIA)

March 10, 2025

Publication History

Revision	Date	Changes Made
Initial	09/20/2013	Original Document
1	N/A	Review and Update
2	09/30/2013	Review and Update
3	03/10/2025	Updated for compliance with E.O. 14168

Privacy Impact Assessment
Financial Investigative Software (FIS)

General Information

1. Name of Project or System.
   Financial Investigative Software (FIS)

2. Describe the project and its purpose or function in the SEC's IT environment.
   The Financial Investigative Software (FIS) is a COTS software product that provides the capability of scanning brokerage and banking statements and allowing for automated reconciliation of the statements. It also provides the capability to extract the data on the statements so it can be analyzed in Access and Excel. The SEC has purchased the FIS software tool to automate and expedite brokerage and bank statement processing and integration into the SEC Enforcement Division (ENF) and the Office of Compliance, Inspections and Examinations (OCIE) systems. The SEC receives customer financial statements in hardcopy or scanned versions in examination and investigation matters. Software is needed to automate the process of converting the data on the statements into an electronic version that can be analyzed. Currently, this is done with time-consuming manual effort.

3. Requested Operational Date? 9/20/13

4. Update: 03/10/2025 - Updated for compliance with E.O. 14168

5. System of Records Notice (SORN) number? SEC-42, Enforcement Files; SEC-55, Information Pertaining or Relevant to SEC Registrants and Their Activities.

5. Is this an Exhibit 300 project or system? ☒ No ☐ Yes

6. What specific legal authorities, arrangements, and/or agreements allow the collection of this information? 15 U.S.C. 77a et seq., 78a et seq., 80a-1 et seq., and 80b-1 et seq.

Specific Questions

SECTION I - Data in the System

1. What data about individuals could be collected, generated, or retained?
   Name, Account number, Credit card number, and Financial information extrapolated from bank statements and brokerage statements.

2. Does the project/system use or collect the social security number (SSN)? (This includes truncated SSNs)
   ☒ No.
   ☐ Yes. If yes, provide the function of the SSN and the legal authority to collect.
3. What are the sources of the data?
   The source of the data being analyzed by FIS is various forms of financial data extrapolated from bank statements and brokerage statements, various financial institutions or from other sources, i.e., parties to a subpoena. This data comes into the Commission in relation to on-going investigations. The data can come in either electronic or hard copy format. If the data is hard copy, it is scanned in house and converted to tiff images. When the data is received, it is processed by ENF's CPU unit then loaded into Recommind.

Once the investigative staff determines the financial data received has value to an investigation, the investigative staff notifies the FIS processing staff and provides copies of the financial data in Recommind to the FIS staff for processing. Once the financial data is processed, an excel spread sheet or .csv file is generated. It is then provided back to the investigative staff for further analysis. The FIS output file assists the investigative staff in evaluating financial data received in an investigation or exam. The spreadsheet is then stored on the J: drive with other case related data.

4. Why is the data being collected?
   The SEC has purchased the FIS software tool to expedite brokerage and bank statement processing and ingestion into the SEC Enforcement Division (ENF) and the Office of Compliance, Inspections and Examinations (OCIE) systems.

5. What technologies will be used to collect the data?
   Documents may be received in hardcopy or electronic format. Hardcopies are scanned and converted to tiff images. The data received is processed by Enforcement's CPU unit and loaded into Recommind. The investigative staff reviews the data received. Data that has investigatory value is copied and provided to the FIS processing staff for processing via FIS. FIS processing staff analyzes the data and generates an excel spreadsheet or .csv file that is provided back to the investigative staff for further analysis. The spreadsheet is then stored on the J: drive with other case related data.

SECTION II - Attributes of the Data (use and accuracy)

1. Describe the uses of the data.
   The data is used by Enforcement in its investigations and OCIE in its exams.

2. Does the system analyze data to assist users in identifying previously unknown areas of note, concern or pattern? ☐ No ☒ Yes If yes, please explain: An analysis of financial data is conducted to determine if the data has investigatory value in an SEC investigation or examination.

3. How will the data collected from individuals or derived by the system be checked for accuracy?
   FIS reconciles the financial statement information and converts it into a standard template format.

SECTION III - Sharing Practices

1. Will the data be shared with any internal organizations?
   ☐ No ☒ Yes If yes, please list organization(s): Could be shared with a limited number of people working on investigations in Enforcement or OCIE.

2. Will the data be shared with any external organizations?
   ☒ No ☐ Yes If yes, please list organizations(s): How is the data transmitted or disclosed to external organization(s)?

3. How is the shared data secured by external recipients?

N/A

4. Does the project/system process or access PII in any other SEC system?
   ☐ No
   ☒ Yes. If yes, list system(s). Recommind

SECTION IV - Notice to Individuals to Decline/Consent Use

1. What privacy notice was provided to the different individuals prior to collection of data? (Check all that apply)
   ☒ Privacy Act Statement ☒ System of Records Notice ☐ Privacy Impact Assessment
   ☐ Web Privacy Policy ☐ Notice was not provided to individuals prior to collection

2. Do individuals have the opportunity and/or right to decline to provide data?
   ☒ Yes ☐ No ☐ N/A
   Please explain: Individuals are provided notice of consent and use at the point of collection, and prior to entering their personal information into Recommind. FIS is fed information from Recommind based on the analysis of the data. (See Section 1.3). This FIS tool does not collect information directly from individuals.

3. Do individuals have the right to consent to particular uses of the data?
   ☒ Yes ☐ No ☐ N/A
   Please explain: Individuals are provided notice of consent and use at the point of collection, and prior to entering their personal information into Recommind. FIS is fed information from Recommind based on the analysis of the data. (See Section 1.3). This FIS tool does not collect information directly from individuals.

SECTION V - Access to Data (administrative and technological controls)

1. Has the retention schedule been established by the National Archives and Records Administration (NARA)?
   ☐ No If no, please explain:
   ☒ Yes If yes, list retention period:
   Records in this system will be retained and disposed of in accordance with a records schedule to be approved by the National Archives and Records Administration.

2. Describe the privacy training provided to users, either generally or specifically relevant to the program or system? All SEC staff and contractors receive annual privacy awareness training, which outlines their roles and responsibilities for properly handling and protecting PII.

3. Has a system security plan been completed for the information system(s) supporting the project?
   ☒ Yes If yes, please provide date C&A was completed: An SEC ATO was issued 9/9/13
   ☐ No If the project does not trigger the C&A requirement, state that along with an explanation

4. Is the system exposed to the Internet without going through VPN?
   ☒ No

☐ Yes If yes, Is secure authentication required? ☐ No ☐ Yes; and
Is the session encrypted? ☐ No ☐ Yes

5. Are there regular (ie. periodic, recurring, etc.) PII data extractions from the system?
☐ No
☒ Yes If yes, please explain: FIS processing staff analyzes the data and generates an excel spreadsheet or .csv file that is provided back to the investigative staff for further analysis. The file is stored on the J: drive with limited access by certain ENF or OCIE staff.

6. Which user group(s) will have access to the system?
A limited number of select operators in the Enforcement and OCIE groups.

7. How is access to the data by a user determined? Access to FIS will be different depending on location. The heavy FIS users in HQ will have the FIS client installed on their local machine. The user will have the FIS client installed on their desktop and from there they will access the DB server, license server and file share. FIS users in the region will not have the application installed locally. These users will RDP into the FIS client, which will be installed on a windows 2008 terminal server (VM). The client on the VM will in turn access the DB server, license server and file share.

   Are procedures documented? ☒ Yes ☐ No

8. How are the actual assignments of roles and rules verified.
All activities performed by FIS processing staff are reviewed. Also, there are auditing measures and controls tied to Active Directory access and activity.

9. What auditing measures/controls and technical safeguards are in place to prevent misuse (e.g., unauthorized browsing) of data? Auditing measures/controls and technical safeguards include Active Directory access control, and logging all login attempts, whether successful or not; all unauthorized events; all activities performed by FIS processing staff; deletion and addition of all cases in FIS.

SECTION VI - Privacy Analysis

Given the amount and type of data being collected, discuss what privacy risks were identified and how they were mitigated.
Privacy risks associated with the collection of the data include potential release to unauthorized users and modification of data by unauthorized personnel. These privacy concerns are mitigated by strictly limiting access to a limited number of select operators in the Enforcement and OCIE groups with a need to know. Additionally, auditing measures are in place to monitor activities of the users of the software.