Federal Trade Commission
Privacy Impact Assessment

Valid8 Financial GovCloud
Forensic Accounting

November 2026

Table of Contents

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

1 System Overview

1.1 Describe the project/system and its purpose.

The Federal Trade Commission (FTC or agency) conducts investigations and litigates cases to accomplish its competition and consumer protection missions. To that effect, the FTC takes law enforcement action against those breaking the law, develops rules to maintain a fair marketplace, conducts research and publishes reports to shed light on important issues, and educates consumers and businesses about their rights and responsibilities.

To identify unfair and deceptive business practices, the FTC Bureau of Consumer Protection (BCP) staff must acquire, process, and analyze financial data in a reasonable amount of time. The agency relies on vendor software that ingests large volumes of financial documents and extracts data from those documents. As such, the FTC has contracted with Valid8 Financial, Inc. for use of their FedRAMP marketplace offering, Valid8 Financial GovCloud. Valid8 Financial GovCloud is cloud-based Software as a Service (SaaS) that specializes in financial analysis using Super Intelligence (SI) and supervised machine learning to extract, parse, read, and analyze data from financial statements accurately and efficiently. Valid8 Financial GovCloud enables the FTC to categorize and reconcile large financial data sets, flag incomplete, incorrect or missing transactions, and conduct forensic accounting activities with the ability to generate interactive data visualizations of information extracted from financial statements.

BCP's forensic accountants and staff analyze financial information to locate assets and maximize recovery in consumer-protection matters, and the division identifies, collects, and preserves electronically stored information (ESI) for use in litigation. Valid8 Financial, Inc. does not collect PII directly from members of the public. Data uploaded to the Valid8 Financial GovCloud system is collected from individuals that are involved in FTC investigations through court orders, responses to administrative subpoenas or civil investigative demands (CIDs), voluntary submissions, and onsite collections.

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

The FTC uses Valid8 Financial GovCloud to collect and maintain information pursuant to the FTC's investigatory, law enforcement, and research authority set forth in the Federal Trade Commission Act, 15 U.S.C. §§ 41 – 58.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check all that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☐ User ID
☐ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☒ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☐ Employment Status, History, or Information
☒ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☒ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☒ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☐ Alias	☐ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☒ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☐ Other *(Please Specify)*:_____
☒ Work Address		
☒ Taxpayer ID		
☒ Credit Card Number		
☒ Facsimile Number		
☒ Medical Information		
☐ Education Records		
☒ Social Security Number		
☐ Mother's Maiden Name		

Note: The FTC does not explicitly collect SSNs for use in Valid8 Financial GovCloud; however, this information may be included in the data that the FTC receives and uploads into the system as part of its investigation and analysis.

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.

Information uploaded to Valid8 Financial GovCloud may consist of financial institution statements that contain monthly account transactions. These statements can typically include account balances, deposits, withdrawals, credits, and fees or interest incurred.

[1] 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.

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

The FTC uploads, maintains, and processes financial information in Valid8 Financial GovCloud to conduct investigations and research in support of the agency's consumer protection and competition missions. When investigating whether companies are engaged in unfair or deceptive practices, staff must obtain evidence of the company's financial practices. This often includes reviewing and analyzing large volumes of data regarding a company's financial accounts. Valid8 Financial GovCloud enables the FTC to categorize and reconcile large financial data sets, flag transactions, and conduct forensic accounting activities. FTC forensic accountants analyze financial information to locate assets and maximize recovery in consumer-protection matters, and identifies, collects, and preserves electronically stored information (ESI) for use in litigation.

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***
FTC Staff	Data uploaded to Valid8 Financial GovCloud is collected from individuals that are involved in FTC investigations through court orders, responses to administrative subpoenas or CIDs, voluntary submissions, and onsite collections. This data includes financial PII relating to consumers or to targets of an investigation. BCP's forensic accountants analyze this financial information in the course of the investigation and/or for law enforcement purposes.
Individual members of the public	The FTC may collect information from individual members of the public who are targets of law enforcement investigations or who engage in activities that are the subject of FTC regulations. This information is collected by serving administrative subpoenas or CIDs, court orders, and voluntary submissions. Valid8 Financial, Inc. does not solicit or collect PII directly from members of the public. PII enters the system only as agency-controlled investigative/evidentiary data placed into the platform by or on behalf of the FTC.
Public records and/or publicly available internet services	The FTC may collect information from public records to support its investigations and research, such as corporate records information and real property ownership. The FTC may also collect information from the web or through mobile applications. This information may be collected by capturing content, data, network protocols, and communications. In addition to collecting information offered for free, the FTC

Source of Data	*Type of Data Provided & How It Is Collected*
	may collect publicly available information through paid services.

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 Staff	BCP forensic accountants and staff use the financial data in Valid8 Financial GovCloud for analysis, organization, and production of ESI during FTC investigations and/or for law enforcement purposes. Only authorized staff have access to data in the system with role-based restrictions and activity logs in place to monitor usage and access.
Valid8 Financial, Inc.	Authorized Valid8 Financial, Inc. staff have role-based access to FTC data in a controlled, centralized manner consistent with least-privilege requirements, in support of forensic platform operations, maintenance, and troubleshooting. FTC data is maintained in a dedicated Amazon Web Services (AWS) account within the Valid8 Financial GovCloud FedRAMP moderate system boundary with logical separation from other tenant environments. FTC data is not used to train Valid8's SI model.

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.

Yes, authorized Valid8 staff have access to FTC data. Valid8 also engages its own subcontractors as part of its Security Operations Center (SOC) provider; SOC personnel hold monitoring accounts scoped to the in-boundary Security Information and Event Management (SIEM) and continuous monitoring functions. All personnel are subject to the following active and passive measures:

- Defined Roles and responsibilities,
- Background checks,
- Separation of duties and least privilege,
- Access requirements and review,
- Logical separation,
- Privacy awareness and role-based training for contractor personnel and
- Annual acknowledgement of Rules of Behavior.

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.

Valid8 personnel are responsible for safeguarding the boundary and security posture of its system. Valid8's subcontractors play an active role in the detection, communication, and reporting of security incidents. All personnel with access are subject to the Incident Response Plan (IRP) of the Valid8 Financial GovCloud system and all access occurs within the controlled boundary and data flows. The IRP covers:

- Roles and responsibilities,
- Event definitions, categorization, and severity,
- Training, preparation, and testing,
- Detection and analysis,
- RCA, breach, and notification procedures,
- Containment, eradication, and recovery procedures, and
- Incident guidelines and process flows.

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.

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

☐ Notice is not provided (explain): _____

Wherever possible, the FTC provides notice to individuals about its policies regarding the use and disclosure of information at the time information is collected. For information that is collected pursuant to a request from the FTC, notice is provided as part of the request (e.g., in a letter request, or in the document outlining the compulsory process request). On those occasions where the FTC cannot provide notice at the time information is collected (e.g., information contained in systems maintained by other organizations), the FTC provides notice via its privacy policy, its Privacy Act system of records notices (SORNs), and its PIAs, including this one.[2] With regard to information collected from internal FTC systems for internal investigations or for the defense of lawsuits brought against the agency, all staff are informed that the agency's computing systems are monitored and that personal information may be collected. Notices are provided to staff at logon, and are also provided in administrative manuals, agency policy documents, and during employee training.

[2] See FTC Privacy Policy, SORNs, and PIAs.

Individuals who provide the FTC with information pursuant to discovery or a related court order are not provided with specific notice by the FTC as to how information will be used or disclosed, other than the FTC's general Privacy Policy and related FAQs. In addition, the use and disclosure of this information is governed by applicable discovery rules and court orders.

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)?

Individuals who provide the FTC with information on a voluntary basis may choose to decline to provide that information. However, individuals do not have a right to decline to provide information that is required by law or that is required to be provided via compulsory process, and refusal to provide the information may result in legal action by the FTC.

Individuals do not typically have a right to consent to particular uses of their information. Data sources who submit their information in FTC law enforcement investigations and mark their submissions confidential, however, may be afforded prior notice and opportunity to object to further disclosure, to the extent provided under Section 21 of the FTC Act and the FTC's Rules of Practice (see, e.g., 16 C.F.R. 4.10 & 4.11).

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

Individuals seeking records about themselves do not have direct access to the Valid8 Financial GovCloud system therefore no privacy risks are associated with the process of providing individuals with access to their own records through the system. Individuals may make a request under the Freedom of Information Act (FOIA) and Privacy Act for access to information maintained about themselves in Valid8 Financial GovCloud or FTC source System of Records. *See* the FTC FOIA and Make a Privacy Act Request websites. For Privacy Act requests, individuals must follow the FTC's Privacy Act rules and procedures, which are published in the Code of Federal Regulations at 16 C.F.R. § 4.13, for requests for information. . However, due to the law enforcement nature of the Privacy Act system that includes the records on the Valid8 Financial GovCloud platform, records in the system about certain individuals, such as defendants, may be exempt from mandatory access by such individuals. See 16 C.F.R. § 4.13(m) (exemptions applicable to certain FTC Privacy Act systems of records). To prevent the risk that records that the agency would be legally required to withhold from public disclosure may be improperly released to an individual purporting to be the subject of such records, the FTC requires additional verification of a requester's identity when such information is reasonably necessary to assure that records are not improperly disclosed.

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 stated above, individuals seeking records about themselves do not have direct access to Valid8 Financial GovCloud. They may make a request under the FOIA and Privacy Act for access to information maintained about themselves in any FTC system. However, due to the law enforcement nature of the applicable Privacy Act system, records in the system about certain individuals, such as defendants, may be exempt from mandatory access by such individuals. See 16 C.F.R. § 4.13(m) (exemptions applicable to certain FTC Privacy Act systems of records). If individuals have questions or concerns about any information in the system, they can raise those questions or concerns in the context of the FTC investigation or litigation in which they are involved.

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?

Data is collected from individuals that are involved in FTC investigations through court orders, voluntary submissions, and onsite collections. The Valid8 Financial GovCloud system has a human-in-the-loop quality assurance review process to ensure faithful representation of this data for faster investigative review. The original documents and data are not altered and stay within the applicable FTC Privacy Act System of Records Notices as set out in section #8.3.

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.

Yes, the Valid8 Financial GovCloud system incorporates both active and passive measures to ensure data is properly accessed and utilized by personnel:

- Defined Roles and responsibilities,
- Separation of duties and least privilege,
- Access requirements and review (FIPS-compliant MFA or Federal Information Processing Standards-compliant multi-factor authentication),
- Logical separation,
- Privacy awareness and role-based training for all personnel,
- Annual acknowledgement of Rules of Behavior,
- Full FIPS at rest and in transit data compliance and
- Continuous monitoring.

All organizations and agencies with access to collected data hold shared responsibility for ensuring its proper use. The Valid8 Financial GovCloud Information System Security Officer is responsible for the ongoing security and privacy posture of the system.

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

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?

Information is received, retained and destroyed/deleted in accordance with applicable FTC policies and procedures and with the National Archives and Records Administration's General Records Schedule 5.2 (Transitory and Intermediary Records), as well as the instructions in the FTC Rules of Practice Section 4.12, Disposition of Documents Submitted to the Commission.

Authorized FTC staff can request the deletion of its data from the Valid8 Financial GovCloud system at any time. Valid8 Financial, Inc. may provide a Certificate of Deletion upon completion of the request.

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.

Authorized FTC staff access Valid8 Financial GovCloud through a secured website that is specifically for the FTC's use. This website is not posted online nor is it made publicly available. The Valid8 Financial GovCloud system uses session cookies solely to maintain authenticated user sessions in the web browser; no tracking cookies are used. Session cookies are transmitted exclusively over connections protected by Transport Layer Security (TLS) 1.2 using FIPS-validated cryptographic modules and are configured with security attributes preventing transmission over unencrypted channels.

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*
Unauthorized disclosure of sensitive financial data	FTC data in the Valid8 Financial GovCloud system may be highly sensitive in nature and includes financial records and identifiers related to individuals in active law enforcement matters. Unauthorized disclosure of this data could result in significant harm and financial injury to individuals as well as compromise FTC investigations. This risk is mitigated by encryption, strict access controls, isolation of FTC data from other tenant data, and documented minimization procedures. There is no public disclosure of FTC data by the Valid8 Financial GovCloud system and approved sub-processors. The platform requires FIPS-compliant MFA authentication to access the system.
Unauthorized alteration or dissemination of information	The Valid8 Financial GovCloud system logs user activity in the system. These logs include successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events. For Web applications, all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes are monitored. Continuous monitoring and reporting are performed by Valid8 and/or its subcontractors.

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

The FTC tenant within the Valid8 Financial GovCloud system incorporates both failed login lockout policy enforcement and an idle session timeout configuration that redirects users to the login page to prevent incidental or malicious exposure or misuse of sensitive data. Five failed login attempts will lead to a lockout of users.

Additionally, SIEM event rules automate the alerting and analysis of potential misuse and breaches leveraging native AWS services, system logs, scanning, and known behavioral correlations. Continuous monitoring rules and coverage are reviewed after any significant changes and annually thereafter.

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).

Valid8 Financial, Inc. does not operate as a system of records retrieved by individual name or other personal identifier under the Privacy Act. Rather, information analyzed and processed via the Valid8 Financial GovCloud system is normally incorporated into FTC nonpublic investigatory files, which are part of the Privacy Act system of records designated as FTC I-1. Additionally, FTC VII-3 -- Computer Systems User Identification and Access Records may also apply.

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?

Although the system does not operate any website that would require the posting of a privacy policy, the collection, use, and disclosure of the information in the system has been reviewed to ensure consistence with the FTC's general Privacy Policy posted on its website.