FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Impact Assessment (PIA)
for
Online Identity Proofing for Members of the Public Interacting with the FDIC

November 17, 2023

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

An FDIC Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) the FDIC collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. The FDIC publishes its PIAs, as well as its System of Records Notices (SORNs), on the FDIC's public-facing website,[1] which describes FDIC's activities that impact privacy, the authority for collecting PII, and the procedures to access and have PII amended or corrected if necessary.

SYSTEM OVERVIEW

The Federal Deposit Insurance Corporation (FDIC) interacts with members of the public in the performance of its mission. Whether helping individuals inquire about deposit insurance coverage, submit a complaint about an FDIC-insured institution, or file a financial claim following a bank failure, the FDIC strives to ensure the people with whom it interacts are who they say they are. FDIC uses Identity Proofing, a concept defined by the National Institute of Standards and Technology (NIST) as "the process for providing sufficient information (e.g., identity history, credentials, documents) to establish an identity," to confirm the identities of those with whom it interacts.

FDIC maintains manual processes where an individual can interact directly with a member of the FDIC team and provide the information necessary to confirm their identity during that interaction. FDIC also uses digital solutions for identity proofing that allow it to better scale its identity proofing activities depending on the circumstances.

FDIC has adopted multiple online identity proofing solutions to verify identities and authenticate members of the public who seek to access to FDIC-provided benefits or services. The online identity proofing (OIP) solutions deployed at FDIC currently include:

- Id.me, a commercial entity that provides secure online identity proofing services to various government agencies and private sector companies; and
- Login.gov, a service administered by the United States General Services Administration (GSA) that provides secure online identity proofing services to various federal agencies.

[1] www.fdic.gov/privacy

The technology used by FDIC for identity proofing processes user information to authenticate and identify the users, which subsequently allows authorized users to access certain FDIC applications and services. The solution provider platforms also collect and maintain data associated with user accounts established and maintained with the solution providers, which, depending upon the solution provider, may be used to facilitate access to other applications and services at other federal agencies or commercial entities beyond the FDIC.

Individuals seeking to use the FDIC applications and services requiring identity proofing start at the application or service front page and then choose the identity proofing solution they wish to use. The user creates an account with the OIP solution, if the user did not already have one, and provides the necessary documentation or evidence to sufficiently verify their identity.[2] Beyond confirmation of the identity, the OIP solution will send only the information necessary to the FDIC application or service to match the identity to the specific-system records.

The FDIC may offer additional choices for online identity proofing in the future, in which case it will update this PIA. Also, FDIC maintains these two options as well as manual processes to ensure individuals have choices with regard to which online identity proofing options they wish to use.

PRIVACY RISK SUMMARY

In conducting this PIA, FDIC identified potential privacy risks, which are summarized below and detailed in the subsequent sections of this PIA. As indicated, recommendations to mitigate those risks were addressed with stakeholders during the assessment. The privacy risks for this system are categorized within the following privacy functional areas:

- Transparency
- Data Quality and Integrity
- Individual Participation

Transparency:

Privacy Risk: Users may not know that they are no longer on the FDIC's website when sent to one of the OIP solution provider sites for identity proofing.

[2] See NIST Special Publication 800-63A, *Digital Identity Guidelines, Enrollment and Identity Proofing Guidelines*, https://pages.nist.gov/800-63-3/sp800-63a.html.

Mitigation: FDIC provides notice to users that they are moving to a third-party's webpage once they click on the OIP solution provider's link. The notice includes a statement that the OIP solution provider is providing the service on FDIC's behalf.

Data Quality and Integrity:

Privacy Risk: A false positive, incorrectly stating that someone is who they purport to be, as part of the identity proofing process could result in fraud and unauthorized access. For example, the FDIC could give the wrong person someone's insurance payout or provide access to the wrong person's records.

Mitigation: Should there be verification issues like false positives, FDIC customer service agents are available to take immediate action to remedy the issue for the individuals affected. In the event the individual is not properly identity-proofed, additional manual processes are available where supplementary identity documentation can be provided directly to FDIC customer service agents. Individuals can also engage FDIC customer service agents directly should they have issues using OIP solution providers. FDIC would follow its Breach Response Plan[3] if personal information was improperly shared. Individuals may also submit privacy complaints[4] in connection with the Corporation's handling of personal information to privacy@fdic.gov.

Additionally, FDIC implements a thorough risk-based approach to security for its systems. FDIC ensures that appropriate security and privacy controls are in place prior to processing information in those systems. FDIC contracts with the OIP solution providers to ensure the effective confirmation of identities for access to FDIC benefits and services, and has mechanisms to hold the contractors accountable if false positives become a problem.

Individual Participation:

Privacy Risk: Individuals may not wish to provide their private identity data, personal documents, or location to specific identity proofing providers.

Mitigation: By offering different OIP solution providers as well as a manual process where individuals can interact directly with FDIC customer service agents, FDIC provides individuals with the ability to choose their preferred identity proofing option.

---

[3] https://www.fdic.gov/policies/privacy/documents/fdic-breach-response-plan.pdf.
[4] https://www.fdic.gov/policies/privacy/request.html.

Section 1.0: Information System

1.1 What information about individuals, including PII (e.g., name, Social Security number, date of birth, address) and non-PII, will be collected, used or maintained in the information system or project?

The OIP solution providers collect various PII elements to verify and authenticate the identity of individuals desiring access to specific FDIC applications and services. The PII elements that may be collected by the OIP solution providers are shown in the following table.

Note that the information collected by the OIP solution providers, as shown in the table below, is not generally shared with FDIC; however, the OIP solution may share a limited amount of information with FDIC if the information is needed to successfully link an individual to the records in an FDIC application. Once the individual has been successfully linked to the records within that application, FDIC will automatically delete the information that was shared by the OIP solution. The OIP solution may also notify the FDIC application or service when user information is updated on the OIP solution system.

Additionally, depending upon the results of the OIP solution authentication, the OIP solution sends a binary assertion back to the FDIC application indicating that the individual either met or did not meet the requirements to be successfully authenticated for authorized access to that application. The binary assertion for the user is maintained within the application and associated with that user's access to the application.

PII Element	ID.me	Login.gov
Full Name	☒	☒
Date of Birth	☒	☒
Place of Birth	☐	☐
Social Security number (SSN)	☒	☒
Employment Status, History or Information	☐	☐
Mother's Maiden Name	☐	☐
Certificates (e.g., birth, death, naturalization, marriage)	☐	☐
Medical Information	☐	☐
Address	☒	☒
Phone Number(s)	☒	☒
Email Address	☒	☒
Employee Identification Number (EIN)	☐	☐

PII Element	ID.me	Login.gov
Financial Information (e.g., checking account #/PINs/passwords, credit report)	☐	☐
Driver's License/State Identification Number	☒	☒
Vehicle Identifiers (e.g., license plates)	☐	☐
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records)	☐	☐
Education Records	☐	☐
Criminal Information	☐	☐
Military Status and/or Records	☐	☐
Investigation Report or Database	☐	☐
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☐
Photographic Identifiers (e.g., image, video) which may only be used if they are included on government issued identification documents provided by the individual during the identity proofing process.	☒	☒
User Information (e.g., User ID, password) User IDs and passwords assigned and maintained by the solution providers.	☒	☒
Passport, passport card, professional certifications/memberships.	☐	☐
Non-driver's license state-issued ID card	☐	☒
IP Address	☒	☒
Geo Location	☒	☐

1.2 What are the sources of the PII in the information system or project?

Data Source	Description of Information Provided by Source
Members of the Public	Members of the public provide their PII to FDIC's OIP solution providers when they create their accounts with the OIP solution providers so that their identities can be verified and authenticated, which enables them to access FDIC applications and services for which they have been authorized access.
Identity Solution Providers	Certain attributes collected by the OIP solution providers may be passed to the FDIC as part of the authentication process. The attributes passed to FDIC will depend on the requirements associated with an FDIC application or service, but the attributes will typically be used to match the identity of the identity-proofed individual to the correct records in those systems. The OIP solution vendors use third-party identity verification entities to confirm documentation provided by system users for identity proofing purposes. Much of this information is

Data Source	Description of Information Provided by Source
	provided directly to the OIP solution by the vendors and not provided by the FDIC.

1.3 Has an Authority to Operate (ATO) been granted for the information system or project?

The ATO for Login.gov was issued on April 23, 2021, and the ATO for ID.me will be issued following the publication of this PIA. Both will be periodically reviewed as part of the FDIC Ongoing Authorization process.

FDIC has not independently assessed all security and privacy controls for either FedRAMP system. FDIC has implemented, tested, and documented all customer-responsible controls for both Login.gov and ID.me and has leveraged FedRAMP and third-party assessment organizations for the remaining security and privacy controls.

Section 2.0: Transparency

Agencies should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

2.1 How does the agency revise its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change?

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC ensures notices are revised to reflect changes in practice or policy that affect PII or changes in activities that may impact privacy as soon as practicable.

2.2 In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this information system or project operate? Provide number and name.

The following SORN applies to the Identity Proofing Solutions: SORN FDIC-041, Personal Information Allowing Network Operations System of Records Notice, which covers individuals that interact with FDIC information technology resources, including FDIC employees, FDIC contractors, FDIC volunteers, FDIC interns, federal and state financial regulator employees, financial institution employees, and other members of the public.

2.3 If the information system or project is being modified, will the Privacy Act SORN require amendment or revision? Explain.

SORN FDIC-041, Personal Information Allowing Network Operations System of Records Notice, does not require amendment or revision. Generally, the FDIC conducts reviews of its SORNs every five years or as needed.

2.4 If a Privacy Act Statement[5] is required, how is the Privacy Act Statement provided to individuals before collecting their PII? Explain.

The requirement for an FDIC Privacy Act Statement is dependent upon the respective FDIC applications that will use OIP solutions to facilitate authorized application access. The FDIC ensures that the forms associated with its applications, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.01 Forms Management Program.

For instance, FDIC applications that leverage an OIP solution will provide individuals with an FDIC Privacy Act Statement at the point they select an OIP solution provider to facilitate access to the application.

Additionally, individuals that select ID.me as their OIP solution provider receive a Privacy Policy on the ID.me website that provides a detailed description about the information ID.me collects, and how it will be used, shared, protected, and how long it will be retained.

Alternatively, users that select Login.gov receive the Login.gov Privacy Practices and Rules of Use on the Login.gov website that describes the information that Login.gov collects, and how it will be used, shared, protected, and how long it will be retained. Additionally, users of Login.gov receive a link to a Privacy Act Statement specific to Login.gov.

2.5 How does the information system or project ensure that its privacy practices are publicly available through organizational websites or otherwise? How does the information system or project ensure that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)? Explain.

---

[5] *See* 5 U.S.C. §552a(e)(3). The Privacy Act Statement provides formal notice to individuals of the authority to collect PII, the purpose for collection, intended uses of the information and the consequences of not providing the information.

The FDIC Privacy Program page provides access to agency SORNs, PIAs, Privacy Policy, and contact information for the SAOP, the Privacy Program Chief, and the Privacy Program (Privacy@fdic.gov). For more information on how FDIC protects privacy, please visit www.fdic.gov/privacy.

Privacy Risk Analysis: Related to Transparency

Privacy Risk: Users may not know that they are no longer on the FDIC's website when sent to one of the OIP solution provider sites for identity proofing.

Mitigation: FDIC provides notice to users that they are moving to a third-party's webpage once they click on the OIP solution provider's link. The notice includes a statement that the OIP solution provider is providing the service on FDIC's behalf.

Section 3.0: Access and Amendment

Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.

3.1 What are the procedures that allow individuals to access their information?

Because the digital identity is maintained for individuals by the OIP solution and not maintained by the FDIC, individuals engage the OIP solution to access their information. Having registered for a user account with an OIP solution, individuals access their information by logging into their OIP solution account.

Individuals can access their information at the same user account they created with the OIP solution. They must provide valid login credentials (username, password, one-time PIN) to login, and if they cannot, then they can contact the respective OIP solutions' customer service process which may allow for manual assistance. Individuals looking to access their information on an FDIC application or service that requires an OIP solution to login may use that login to access their information or may contact FDIC customer service.

3.2 What procedures are in place to allow the individuals to correct inaccurate or erroneous information?

Because the digital identity is maintained for individuals by the OIP solution and not maintained by the FDIC, individuals engage the OIP solution to access and correct their information. Having registered for a user account with an OIP solution,

individuals access their information by logging into their OIP solution account. After logging into the OIP solution, individuals may make changes to their information.

Depending upon the FDIC applications, some personal information collected by an OIP solution may be shared with FDIC applications as deemed necessary and appropriate by authorized parties within the FDIC. In those instances, changes or updates made by individuals to that personal information maintained by the OIP solution will be shared by the OIP solution with the FDIC application.

3.3 How does the information system or project notify individuals about the procedures for correcting their information?

Because the digital identity is maintained for individuals by the OIP solution and not maintained by the FDIC, individuals engage the OIP solution for procedures for correcting their information.

ID.me users receive notice on how they may correct or change their information in the ID.me Privacy Policy available from the ID.me website, while Login.gov users are provided notice on how they may correct or change their information in the Login.gov Privacy and Security Policy, which is accessible from login page of the Login.gov website.

Privacy Risk Analysis: Related to Access and Amendment

Privacy Risk: There are no identifiable privacy risks related to access and amendment for OIP solutions.

Mitigation: No mitigation actions are recommended.

Section 4.0: Accountability

Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

4.1 Describe how FDIC's governance and privacy program demonstrates organizational accountability for and commitment to the protection of individual privacy.

FDIC maintains a risk-based, enterprise-wide privacy program that is based upon sound privacy practices. The FDIC Privacy Program is compliant with all applicable laws and is designed to build and sustain public trust, protect and minimize the impacts on the privacy of individuals, while also achieving the FDIC's mission.

The FDIC Privacy Program is led by the FDIC's Chief Information Officer (CIO) and Chief Privacy Officer (CPO), who also has been designated as FDIC's Senior Agency Official for Privacy (SAOP). The CIO/CPO reports directly to the FDIC Chairman, and is responsible for ensuring compliance with applicable federal privacy requirements, developing and evaluating privacy policy, and managing privacy risks. The program ensures compliance with federal privacy law, policy, and guidance. This includes the Privacy Act of 1974, as amended; Section 208 of the E-Government Act of 2002; Section 522 of the 2005 Consolidated Appropriations Act; Federal Information Security Modernization Act of 2014; Office of Management and Budget (OMB) privacy policies; and standards issued by the National Institute of Standards and Technology (NIST).

The FDIC's Privacy Program supports the SAOP in the management and execution of the FDIC's Privacy Program.

4.2 Describe the FDIC privacy risk management process that assesses privacy risks to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

Risk analyses are an integral component of FDIC's Privacy Program. Privacy risks for new and updated collections of PII are analyzed and documented in Privacy Threshold Analyses (PTAs) and Privacy Impact Assessments (PIAs). The Privacy Program looks across all FDIC systems and programs to identify potential areas of privacy risk. The PTA is used to assess systems or sub-systems, determine privacy compliance requirements, categorize systems, and determine which privacy controls should be assessed for each system.

4.3 Does this PIA capture privacy risks posed by this information system or project in accordance with applicable law, OMB policy, or any existing organizational policies and procedures?

Yes, this PIA captures privacy risks posed by OIP solutions through the privacy risk analysis sections throughout the document. PIAs are posted on FDIC's public-facing

website, https://www.fdic.gov/privacy.

4.4 What roles, responsibilities and access will contractors have with the design and maintenance of the information system or project?

Contractors are employed by the FDIC's Division of Information Technology (DIT) to provide development and maintenance support for the integration of OIP solutions with FDIC applications and services.

Due to contractors' access to PII, contractors take mandatory annual information security and privacy training. Privacy and security-related responsibilities are specified in contracts and associated Risk Level Designation documents. Privacy-related roles, responsibilities, and access requirements are documented in relevant PIAs.

4.5 Has a Contractor Confidentiality Agreement or a Non-Disclosure Agreement been completed and signed for contractors who work on the information system or project? Are privacy requirements included in the contract?

Yes, appropriate Confidentiality Agreements have been completed and signed for contractors who support the OIP solutions. Privacy and security requirements for contractors and service providers are mandated and are documented in relevant contracts.

4.6 How is assurance obtained that the information in the information system or project is used in accordance with the practices described in this PIA and, if applicable, the associated Privacy Act System of Records Notice?

Through the conduct, evaluation and review of PIAs and SORNs, the FDIC monitors and audits privacy controls. Internal privacy policies are reviewed and updated as required. The FDIC Privacy Program implements a Privacy Continuous Monitoring (PCM) program in accordance with OMB Circular A-130.

4.7 Describe any privacy-related training (general or specific) that is provided to users of this information system or project.

Annual Security and Privacy Training is mandatory for all FDIC employees and contractors and they are required to electronically certify their acceptance of responsibilities for privacy requirements upon completion. Specified role-based privacy training sessions are planned and provided by the FDIC Privacy Program as well.

4.8 Describe how the FDIC develops, disseminates, and updates reports to the Office of Management and Budget (OMB), Congress, and other oversight bodies, as appropriate, to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

The FDIC Privacy Program develops reports both for internal and external oversight bodies through several methods, including the Annual Senior Agency Official for Privacy (SAOP) Report as required by FISMA, and regular reporting to the SAOP, the CISO, and the Information Technology Risk Advisory Committee.

4.9 Explain how this information system or project protects privacy by automating privacy controls?

The OIP solutions are used to facilitate access to various FDIC applications that are authorized to collect PII. The respective PIAs and SORNs for those applications identify how the systems protect privacy by automating privacy controls. FDIC's PIAs and SORNs are posted on FDIC's public-facing website, https://www.fdic.gov/privacy.

Privacy has been integrated within the FDIC Systems Development Life Cycle (SDLC), ensuring that stakeholders are aware of, understand, and address Privacy requirements throughout the SDLC, including the automation of privacy controls when possible. Additionally, FDIC has implemented technologies to track, respond, remediate, and report on breaches, as well as to track and manage PII inventory.

4.10 Explain how this information system or project maintains an accounting of disclosures held in each system of records under its control, including: (1) Date, nature, and purpose of each disclosure of a record; and (2) Name and address of the person or agency to which the disclosure was made?

The FDIC maintains an accurate accounting of disclosures of information held in each system of record under its control, in accordance with the Privacy Act of 1974 and 12 C.F.R. § 310. Disclosures are tracked and managed using the FDIC FOIA solution.

4.11 Explain how the information system or project retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer?

The FDIC retains the accounting of disclosures as specified by the Privacy Act of 1974 and 12 C.F.R. § 310.

4.12 Explain how the information system or project makes the accounting of disclosures available to the person named in the record upon request?

The FDIC makes the accounting of disclosures available to the person named in the record upon request as specified by the Privacy Act of 1974 and 12 C.F.R. § 310.

Privacy Risk Analysis: Related to Accountability

Privacy Risk: There are no identifiable risks associated with Accountability.

Mitigation: No mitigation actions are recommended.

Section 5.0: Authority

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.

5.1 Provide the legal authority that permits the creation, collection, use, processing, storage, maintenance, dissemination, disclosure and/or disposing of PII within the information system or project.

The FDIC ensures that collections of PII are legally authorized through the conduct and documentation of PIAs and the development and review of SORNs. FDIC Circular 1360.20, "Privacy Program," mandates that the collection of PII be in accordance with Federal laws and guidance. The OIP solutions collect PII pursuant to the following laws and regulations:

- Section 9 of the Federal Deposit Insurance Act (12 U.S.C. § 1819) and
- Executive Order 13681—Improving the Security of Consumer Financial Transactions.

Additionally, the OIP solutions are used to facilitate access to various FDIC applications that are authorized to collect PII. The respective PIAs and SORNs for those applications identify their authorization to collect PII. FDIC's PIAs and SORNs are posted on FDIC's public-facing website, https://www.fdic.gov/privacy.

Privacy Risk Analysis: Related to Authority

Privacy Risk: There are no identifiable risks associated with Authority.

Mitigation: No mitigation actions are recommended.

Section 6.0: Minimization

Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.

6.1 How does the information system or project ensure that it has identified the minimum PII that are relevant and necessary to accomplish the legally authorized purpose of collection?

The OIP solution providers facilitate access to various FDIC applications. The PIAs and SORNs, as appropriate, for those FDIC applications identify the minimum PII that is relevant and necessary to accomplish the legally authorized purpose for which the PII associated with that application is collected. FDIC's PIAs and SORNs are posted on FDIC's public-facing website, https://www.fdic.gov/privacy.

Through the conduct, evaluation, and review of the privacy artifacts[6] for the OIP solution providers, FDIC has ensured that the collection of PII by the OIP solution providers is relevant and necessary to accomplish the legally authorized purpose for which it is collected.

6.2 How does the information system or project ensure limits on the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent?

The collection and retention of records by OIP solution providers is dependent upon their respective legal, contractual or internal policy requirements.

FDIC applications that leverage OIP solutions will provide individuals with an FDIC Privacy Act Statement that allows individuals to make an informed decision about whether they want to share their information with an OIP solution provider. FDIC's

[6] Privacy artifacts include Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and System of Record Notices (SORN).

Privacy Act Statements provide the authority, purpose, and routine uses describing how an individual's information may be shared.

Additionally, individuals that select ID.me as their OIP solution provider receive a Privacy Policy on the ID.me website that provides a detailed description about the information ID.me collects, and how it will be used, shared, protected, and how long it will be retained.

Alternatively, users that select Login.gov receive the Login.gov Privacy Practices and Rules of Use on the Login.gov website that describes the information that Login.gov collects, and how it will be used, shared, protected, and how long it will be retained. Additionally, users of Login.gov receive a link to a Privacy Act Statement specific to Login.gov.

6.3 How often does the information system or project evaluate the PII contained in the information system or project to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose?

The FDIC maintains an inventory of systems that contain PII, including those that are supported by OIP solution providers. The Privacy Program reviews information in the systems at the frequency defined in the FDIC Information Security Continuous Monitoring Strategy. New collections are evaluated to determine if they should be added to the inventory.

6.4 What are the retention periods of the data in this information system or project? What are the procedures for disposition of the data at the end of the retention period? Under what guidelines are the retention and disposition procedures determined? Explain.

The record retention periods for data collected by OIP solution providers is dependent upon their respective legal, contractual, or internal policy requirements. Individuals that select ID.me as their OIP solution receive a Privacy Policy on the ID.me website that provides a detailed description about the information ID.me collects, and how it will be used, shared, protected, and how long it will be retained.

Alternatively, users that select Login.gov receive the Login.gov "Privacy Practices and Rules of Use" notice on the Login.gov website that describes the information that Login.gov collects, and how it will be used, shared, protected, and how long it will be retained. Additionally, users of Login.gov receive a Privacy Act Statement specific to

Login.gov, where users are provided a link to the Login.gov SORN,[7] which also offers users a detailed description about the information Login.gov collects, and how it will be used, shared, protected, and how long it will be retained.

Depending upon the FDIC application, some personal information collected by an OIP solution provider may be shared with the FDIC application as deemed necessary and appropriate by FDIC. In those instances, information that is shared with an FDIC application and maintained by the FDIC application will follow the records retention schedule associated with that application. The records schedule for FDIC applications that leverage OIP solutions are available in the PIAs and SORNs for those applications. FDIC's PIAs and SORNs are posted on FDIC's public-facing website, https://www.fdic.gov/privacy.

Generally, FDIC records are retained in accordance with the FDIC Circular 1210.01, "Records and Information Management Program," which is informed by the Federal Records Act and NARA regulations Management Policy Manual and NARA-approved record retention schedule. Information related to the retention and disposition of data is captured and documented within the PIA process. The retention and disposition of records, including PII, is addressed in Circulars 1210.01 and 1360.09, "Protecting Information."

6.5 What are the policies and procedures that minimize the use of PII for testing, training, and research? Does the information system or project implement controls to protect PII used for testing, training, and research?

The FDIC has developed an enterprise test data strategy to reinforce the need to mask or use synthetic data in the lower environments whenever possible, and ensure all environments are secured appropriately based on the impact level of the information and the information system.

The OIP solutions provide specifics on whether users' data may be used for testing, training, and research in their respective privacy policies.

Privacy Risk Analysis: Related to Minimization

Privacy Risk: There are no identifiable privacy risks related to minimization for OIP solutions.

Mitigation: No mitigation actions are recommended.

[7] https://www.federalregister.gov/documents/2022/11/21/2022-25420/privacy-act-of-1974-notice-of-a-modified-system-of-records.

Section 7.0: Data Quality and Integrity

Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

7.1 Describe any administrative and technical controls that have been established to ensure and maximize the quality, utility, and objectivity of PII, including its accuracy, relevancy, timeliness, and completeness.

The FDIC maintains an inventory of systems that contain PII, which includes those supported by OIP solution providers. The Privacy Program reviews privacy artifacts for adequate controls to ensure the accuracy, relevance, timeliness, and completeness of PII in each instance of collection or creation.

The administrative and technical controls established by the respective OIP solution providers is dependent upon their respective legal, contractual, or internal policy requirements. Individuals that select ID.me as their OIP solution provider receive a Privacy Policy on the ID.me website that provides a detailed description of administrative and technical controls that have been implemented by ID.me.

Alternatively, users that select Login.gov as their OIP solution provider receive the Login.gov "Privacy Practices and Rules of Use" notice and the Login.gov "Our Security Practices" notice on the Login.gov website that describes the administrative and technical controls established by Login.gov.

7.2 Does the information system or project collect PII directly from the individual to the greatest extent practicable?

The OIP solution providers collect PII directly from the individual, and validate that information with the issuing sources (e.g., state DMVs) or authoritative sources (e.g., credit bureaus). Those issuing and authoritative sources indicate to the OIP solution providers whether they were able to validate the information or not.

Depending upon the FDIC application, some personal information collected by an OIP solution provider may be shared with the FDIC application as deemed necessary and appropriate by authorized parties within the FDIC. Additionally, once an individual has obtained access to an FDIC application via an OIP solution provider, additional personal information may be collected from the individual for use by that application.

The Privacy Program reviews application-specific privacy artifacts for adequate controls to ensure that PII is collected directly from the individual to the greatest extent practicable.

7.3 Describe any administrative and technical controls that have been established to detect and correct PII that is inaccurate or outdated.

The administrative and technical controls established by the respective OIP solution providers is dependent upon their respective legal, contractual or internal policy requirements. Individuals that select ID.me as their OIP solution provider receive a Privacy Policy on the ID.me website that provides a detailed description of administrative and technical controls that have been implemented by ID.me.

Alternatively, users that select Login.gov as their OIP solution provider receive the Login.gov "Privacy Practices and Rules of Use" notice and the Login.gov "Our Security Practices" notice on the Login.gov website, as well as the Login.gov Privacy Impact Assessment that describes the administrative and technical controls established by Login.gov.

The FDIC maintains an inventory of systems that contain PII, which includes those supported by OIP solution providers. The Privacy Program reviews application-specific privacy artifacts to ensure adequate controls are in place for those applications to check for and correct any inaccurate or outdated PII in its inventory

7.4 Describe the guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

The administrative and technical controls established by the respective OIP solution providers is dependent upon their respective legal, contractual or internal policy requirements. Individuals that select ID.me as their OIP solution provider receive a Privacy Policy on the ID.me website that provides a detailed description of controls implemented by ID.me with respect to the quality, utility, objectivity, and integrity of disseminated information.

Alternatively, users that select Login.gov as their OIP solution provider receive the Login.gov "Privacy Practices and Rules of Use" notice and the Login.gov "Our Security Practices" notice on the Login.gov website, as well as the Login.gov Privacy Impact Assessment that describes the controls implemented by Login.gov with respect to the quality, utility, objectivity, and integrity of disseminated information.

The FDIC maintains an inventory of systems that contain PII, which includes those supported by OIP solution providers. The Privacy Program reviews application-specific

privacy artifacts to ensure adequate controls are in place for those applications to check for quality, utility, objectivity, and integrity of disseminated information.

Additionally, the FDIC's guidelines for the disclosure of information subject to Privacy Act protections are found in Part 310 of the FDIC Rules and Regulations.

7.5 Describe any administrative and technical controls that have been established to ensure and maximize the integrity of PII through security controls.

The administrative and technical controls established by the respective OIP solution providers is dependent upon their respective legal, contractual or internal policy requirements. Individuals that select ID.me as their OIP solution provider receive a Privacy Policy on the ID.me website that provides a detailed description of administrative and technical controls that have been implemented by ID.me to ensure the integrity of PII.

Alternatively, users that select Login.gov as their OIP solution provider receive the Login.gov "Privacy Practices and Rules of Use" notice and the Login.gov "Our Security Practices" notice on the Login.gov website, as well as the Login.gov Privacy Impact Assessment that describes the administrative and technical controls established by Login.gov to ensure the integrity of PII.

The FDIC maintains an inventory of systems that contain PII, which includes those supported by OIP solution providers. The Privacy Program reviews application-specific privacy artifacts to ensure adequate controls are in place for those applications to ensure the integrity of PII.

7.6 Does this information system or project necessitate the establishment of a Data Integrity Board to oversee a Computer Matching Agreements and ensure that such an agreement complies with the computer matching provisions of the Privacy Act?

The FDIC does not maintain any Computer Matching Agreements under the Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988. Consequently, the FDIC does not need to establish a Data Integrity Board.

Privacy Risk Analysis: Related to Data Quality and Integrity

Privacy Risk: A false positive, incorrectly stating that someone is who they purport to be, as part of the identity proofing process could result in fraud and unauthorized access. For

example, the FDIC could give the wrong person someone's insurance payout or provide access to the wrong person's records.

Mitigation: Should there be verification issues like false positives, FDIC customer service agents are available to take immediate action to remedy the issue for the individuals affected. In the event the individual is not properly identity-proofed, additional manual processes are available where supplementary identity documentation can be provided directly to FDIC customer service agents. Individuals can also engage FDIC customer service agents directly should they have issues using OIP solution providers. FDIC would follow its Breach Response Plan[8] if personal information was improperly shared. Individuals may also submit privacy complaints[9] in connection with the Corporation's handling of personal information to privacy@fdic.gov.

Additionally, FDIC implements a thorough risk-based approach to security for its systems. FDIC ensures that appropriate security and privacy controls are in place prior to processing information in those systems. FDIC contracts with the OIP solution providers to ensure the effective confirmation of identities for access to FDIC benefits and services, and has mechanisms to hold the contractors accountable if false positives become a problem.

Section 8.0: Individual Participation

Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

8.1 Explain how the information system or project provides means, when feasible and appropriate, for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection.

The FDIC ensures that the forms associated with its applications, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.01 "Forms Management Program." FDIC applications that leverage an OIP solution will provide individuals with an FDIC Privacy Act Statement once they select an OIP solution provider to facilitate access to the application.

[8] https://www.fdic.gov/policies/privacy/documents/fdic-breach-response-plan.pdf.
[9] https://www.fdic.gov/policies/privacy/request.html.

Additionally, individuals that select ID.me as their OIP solution provider receive a Privacy Policy on the ID.me website that provides notice to individuals about the information ID.me collects, and how it will be used, shared, protected, and how long it will be retained.

Alternatively, users that select Login.gov receive the Login.gov Privacy Practices and Rules of Use on the Login.gov website that provides notice to individuals about the information that Login.gov collects, and how it will be used, shared, protected, and how long it will be retained. Additionally, users of Login.gov receive a link to a Privacy Act Statement specific to Login.gov.

8.2 Explain how the information system or project provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII.

The FDIC ensures that the forms associated with its applications, whether paper-based or electronic, that collect PII display an appropriate Privacy Act Statement in accordance with the Privacy Act of 1974 and FDIC Circular 1213.01 "Forms Management Program." FDIC applications that leverage an OIP solution will provide individuals with an FDIC Privacy Act Statement once they select an OIP solution provider to facilitate access to the application. The Privacy Act Statement provides the consequences for providing authorization to collect, use, disseminate, and retain their PII.

Additionally, individuals that select ID.me as their OIP solution provider receive a Privacy Policy on the ID.me website that provides notice to individuals about the information ID.me collects, and how it will be used, shared, protected, and how long it will be retained, as well as the consequences of an individual's approving or declining the authorization of the collection, use, dissemination, and retention of their PII.

Alternatively, users that select Login.gov receive the Login.gov Privacy Practices and Rules of Use on the Login.gov website that provides notice to individuals about the information that Login.gov collects, and how it will be used, shared, protected, and how long it will be retained. Additionally, users of Login.gov receive a link to a Privacy Act Statement specific to Login.gov that describes the consequences of an individual's approving or declining the authorization of the collection, use, dissemination, and retention of their PII.

8.3 Explain how the information system or project obtains consent, when feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII.

It is not feasible or appropriate to get direct consent prior to any new use or disclosures of previously collected PII. If applicable, the FDIC Privacy Program will update the relevant SORN(s) as well as the relevant PIA.

8.4 Explain how the information system or project ensures that individuals are aware of and, when feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the FDIC collected the PII.

The FDIC applications supported by OIP solution providers only use PII for the purpose listed in Section 9.1 of this PIA and the various PIAs for FDIC applications supported by OIP solution providers. The FDIC ensures that individuals are aware of all uses of PII not initially described in the public notice, at the time of collection, in accordance with the Privacy Act of 1974 and the FDIC Privacy Policy.

Additionally, individuals that select ID.me as their OIP solution provider receive a Privacy Policy on the ID.me website that provides notice to individuals about the information ID.me collects, and how it will be used, shared, protected, and how long it will be retained, as well as the consequences of an individual's approving or declining the authorization of the collection, use, dissemination, and retention of their PII.

Alternatively, users that select Login.gov receive the Login.gov Privacy Practices and Rules of Use on the Login.gov website that provides notice to individuals about the information that Login.gov collects, and how it will be used, shared, protected, and how long it will be retained. Additionally, users of Login.gov receive a link to a Privacy Act Statement specific to Login.gov that describes the consequences of an individual's approving or declining the authorization of the collection, use, dissemination, and retention of their PII.

8.5 Describe the process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices?

The FDIC Privacy Program website, http://www.fdic.gov/privacy/, instructs individuals to direct privacy questions to the FDIC Privacy Program through the Privacy@fdic.gov email address. Complaints and questions are handled on a case-by-case basis.

Privacy Risk Analysis: Related to Individual Participation

Privacy Risk: Individuals may not wish to provide their private identity data, personal documents, or location to specific identity proofing providers.

Mitigation: By offering different OIP solution providers as well as a manual process where individuals can interact directly with FDIC customer service agents, FDIC provides individuals with the ability to choose their preferred identity proofing option.

Section 9.0: Purpose and Use Limitation

Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

9.1 Describe the purpose(s) for which PII is collected, used, maintained, and shared as specified in the relevant privacy notices.

FDIC uses OIP solutions to verify identities and authenticate individuals who seek authorized access to various FDIC applications. The respective PIAs and SORNs for those applications that leverage OIP solution providers describe the purpose(s) for which they collect PII and how it is used, maintained, and shared. FDIC's PIAs and SORNs are posted on FDIC's public-facing website, https://www.fdic.gov/privacy.

Additionally, individuals that select ID.me as their OIP solution provider receive a Privacy Policy on the ID.me website that provides notice to individuals about the information ID.me collects, and how it will be used, shared, protected, and how long it will be retained, as well as the consequences of an individual's approving or declining the authorization of the collection, use, dissemination, and retention of their PII.

Alternatively, users that select Login.gov receive the Login.gov Privacy Practices and Rules of Use on the Login.gov website that provides notice to individuals about the information that Login.gov collects, and how it will be used, shared, protected, and how long it will be retained. Additionally, users of Login.gov receive a link to a Privacy Act Statement specific to Login.gov that describes the consequences of an individual's approving or declining the authorization of the collection, use, dissemination, and retention of their PII.

9.2 Describe how the information system or project uses PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices? Who is responsible for assuring proper use of data in the information system or project and, if applicable, for determining what data can be shared with other parties and information systems? Have policies and procedures been established for this

responsibility and accountability? Explain.

Through the conduct, evaluation, and review of privacy artifacts, and in conjunction with the implementation of applicable privacy controls, the FDIC ensures that PII is only used for authorized uses internally in accordance with the Privacy Act and FDIC Circular 1360.09 "Protecting Information." Additionally, annual Information Security and Privacy Awareness Training is mandatory for all employees and contractors, which includes information on rules and regulations regarding the sharing of PII with third-parties.

9.3 How is access to the data determined and by whom? Explain the criteria, procedures, security requirements, controls, and responsibilities for granting access.

Access to the data collected and maintained by Login.gov is granted and controlled as described in the GSA Login.gov PIA,[10] while access to the data collected and maintained by ID.me is granted and controlled as described in the ID.me Privacy Policy.

Generally, access to FDIC applications, including those that leverage OIP solution providers, is granted on a need-to-know basis. FDIC follows Guidelines established in the Corporation's Access Control Policies and Procedures document. Controls are documented in the system documentation and a user's access is tracked in the Corporation's access control tracking system.

9.4 Do other internal information systems receive data or have access to the data in the information system? If yes, explain.

The OIP solution providers are used by FDIC to verify identities and authenticate individuals who seek authorized access to various FDIC applications. It depends upon the respective FDIC applications as to whether they provide data or application access to other internal FDIC internal information systems. The respective PIAs and SORNs for those applications will indicate if or how they share information with other internal FDIC applications.

Regarding ID.me, the ID.me Privacy Policy available from the ID.me website describes the information ID.me collects, and how it will be used, shared, protected, and how long it will be retained. Alternatively, regarding Login.gov, the Login.gov PIA available from the Login.gov website describes the information Login.gov collects, and how it will be used, shared, protected, and how long it will be retained.

[10] https://www.gsa.gov/system/files/Login.gov_.pdf

9.5 Will the information system or project aggregate or consolidate data in order to make determinations or derive new data about individuals? If so, what controls are in place to protect the newly derived data from unauthorized access or use?

FDIC uses OIP solutions to verify identities and authenticate individuals who seek authorized access to various FDIC applications. It is dependent upon the respective FDIC applications as to whether they aggregate or consolidate data in order to make determinations or derive new data about individuals. The respective PIAs for those applications will indicate what controls are in place to protect newly derived data from unauthorized access or use.

With respect to ID.me, the ID.me Privacy Policy describes how ID.me may derive information about its users and how the information ID.me collects is used, shared, protected, and how long it will be retained. Alternatively, the Login.gov PIA addresses how Login.gov user data is aggregated and how the information Login.gov collects is used, shared, protected, and how long it will be retained.

9.6 Does the information system or project share PII externally? If so, is the sharing pursuant to a Memorandum of Understanding, Memorandum of Agreement, or similar agreement that specifically describes the PII covered and enumerates the purposes for which the PII may be used? Please explain.

FDIC uses OIP solutions to verify identities and authenticate individuals who seek authorized access to various FDIC applications. It is dependent upon the respective FDIC applications as to whether they share PII externally from the application. The respective PIAs for those applications will indicate what controls in place around the sharing of information external to those applications.

Through the conduct, evaluation, and review of PIAs and SORNs, the FDIC ensures that PII shared with third-parties is used only for the authorized purposes identified or for a purpose compatible with those purposes, in accordance with the Privacy Act of 1974, and FDIC Circular 1360.20 “Privacy Program.” The FDIC also ensures that agreements regarding the sharing of PII with third-parties specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used, in accordance with FDIC Circular 1360.09.

With respect to ID.me, the ID.me Privacy Policy describes how ID.me may share information about its users external to ID.me and how the information ID.me collects is used, protected, and how long it will be retained. Alternatively, the Login.gov Privacy Act Statement, Login.gov PIA, and Login.gov SORN address how the

information Login.gov collects is shared and how the information is used, protected, and how long it will be retained.

9.7 Describe how the information system or project monitors, audits, and trains its staff on the authorized sharing of PII with third-parties and on the consequences of unauthorized use or sharing of PII.

Annual Information Security and Privacy Awareness Training is mandatory for all FDIC employees and contractors, which includes information on rules and regulations regarding the sharing of PII with third-parties.

FDIC uses OIP solutions to verify identities and authenticate individuals who seek authorized access to various FDIC applications. It is dependent upon the respective FDIC applications as to whether they share PII externally from the application. The respective PIAs for those applications will indicate what controls in place around the sharing of information external to those applications.

With respect to ID.me, the ID.me Privacy Policy describes how ID.me may share information about its users external to ID.me and how the information ID.me collects is used, protected, and how long it will be retained. Alternatively, the Login.gov Privacy Act Statement, Login.gov PIA, and Login.gov SORN address how the information Login.gov collects is shared and how the information is used, protected, and how long it will be retained.

9.8 Explain how the information system or project evaluates any proposed new instances of sharing PII with third-parties to assess whether the sharing is authorized and whether additional or new public notice is required.

The FDIC reviews privacy artifacts to evaluate any proposed new instances of sharing PII with third-parties to assess whether the sharing is authorized and whether additional or new public notice is required.

With respect to ID.me, the ID.me Privacy Policy describes how ID.me may share information about its users external to ID.me and how the information ID.me collects is used, protected, and how long it will be retained. Alternatively, the Login.gov Privacy Act Statement, Login.gov PIA, and Login.gov SORN address how the information Login.gov collects is shared and how the information is used, protected, and how long it will be retained. It is the responsibility of the OIP solution providers to evaluate new instances of sharing PII with third-parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Privacy Risk Analysis: Related to Use Limitation

Privacy Risk: There are no identifiable privacy risks related to use limitation for OIP solutions.

Mitigation: No mitigation actions are recommended.

Section 10.0: Security

Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

10.1 Describe the process that establishes, maintains, and updates an inventory that contains a listing of all information systems or projects identified as collecting, using, maintaining, or sharing PII.

The FDIC Privacy Program maintains an inventory of all programs and information systems identified as collecting, using, maintaining, or sharing PII.

10.2 Describe the process that provides each update of the PII inventory to the CIO or information security official to support the establishment of information security requirements for all new or modified information systems or projects containing PII?

The FDIC Privacy Program updates the CISO on PII holdings via the PTA adjudication process. As part of the PTA adjudication process, the FDIC Privacy Program reviews the system or project's FIPS 199 determination. The FDIC Privacy Program will recommend the appropriate determination to the CISO should the potential loss of confidentiality be expected to cause a serious adverse effect on individuals.

10.3 Has a Privacy Incident Response Plan been developed and implemented?

FDIC has developed and implemented a Breach Response Plan in accordance with OMB M-17-12.

10.4 How does the agency provide an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan?

Responses to privacy breaches are addressed in an organized and effective manner in accordance with the FDIC's Breach Response Plan.

Privacy Risk Analysis: Related to Security

Privacy Risk: There are no identifiable privacy risks related to security for OIP solutions.

Mitigation: No mitigation actions are recommended.