Office of Personnel Management.

Kayyonne Marston,

Federal Register Liaison.

[FR Doc. 2024–16477 Filed 7–25–24; 8:45 am]

BILLING CODE 6325–39–P

POSTAL SERVICE

Privacy Act of 1974; System of Records

AGENCY: Postal Service®.

ACTION: Notice of a modified system of records.

SUMMARY: The United States Postal Service® (USPS®) is proposing to revise three Customer Privacy Act Systems of Records (SOR). These modifications are being made to provide further identity verification services for business customers and to mitigate fraud.

DATES: These revisions will become effective without further notice on August 26, 2024, unless, in response to comments received on or before that date result in a contrary determination.

ADDRESSES: Comments may be submitted via email to the Privacy and Records Management Office, United States Postal Service Headquarters (*uspsprivacyfedregnotice@usps.gov*). To facilitate public inspection, arrangements to view copies of any written comments received will be made upon request.

FOR FURTHER INFORMATION CONTACT: Janine Castorina, Chief Privacy and Records Management Officer, Privacy and Records Management Office, 202–268–3069 or *uspsprivacyfedregnotice@usps.gov*.

SUPPLEMENTARY INFORMATION: This notice is in accordance with the Privacy Act requirement that agencies publish their systems of records in the **Federal Register** when there is a revision, change, or addition, or when the agency establishes a new system of records. The Postal Service has determined that Customer Privacy Act System of Records USPS 810.100 *www.usps.com* Registration, USPS 860.000 Financial Transactions, and USPS 910.000 Identity and Document Verification Services, should be revised to provide further identity verification services for business customers and to mitigate fraud.

I. Background

As the Postal Service continues its mission to serve the people of the United States, it continues to innovate to find products and solutions that will benefit its customers. To this end, USPS has introduced the Business Customer Gateway, a platform that allows businesses of all types quick and easy access to postal services. As part of this initiative, to protect the safety of its customers and to combat fraudulent activity, Business Customers will be required to provide their Employer Identification Number (EIN) when registering for an account. This EIN will be processed through USPS' existing identity verification methodology to validate these accounts, further enhancing the security of these new systems.

II. Rationale for Changes to USPS Privacy Act Systems of Records

The Postal Service will modify three Privacy Act Systems of Records accordingly to implement these changes:

USPS 810.100 will update category of records 1 and 2 to include Employer Identification Number (EIN)

USPS 860.000 will include a new purpose, 5, and will update category of records 1 to include Employer Identification Number (EIN)

USPS 910.000 will update category of records 1 to include Employer Identification Number (EIN)

III. Description of the Modified System of Records

Pursuant to 5 U.S.C. 552a(e)(11), interested persons are invited to submit written data, views, or arguments on this proposal. A report of the proposed revisions to this SOR has been sent to Congress and to the Office of Management and Budget for their evaluations. The Postal Service does not expect this modified system of records to have any adverse effect on individual privacy rights. Accordingly, for the reasons stated above, the Postal Service proposes revisions to this system of records. SORs 810.100 *www.usps.com* Registration, Financial Transactions 860.000, and 910.000 Identity and Document Verification are provided below in their entirety.

SYSTEM NAME AND NUMBER:

USPS 810.100, *www.usps.com* Registration.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

Computer Operations Service Centers.

SYSTEM MANAGER(S):

Chief Customer and Marketing Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260–5005, (202) 268–7536.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

39 U.S.C. 401, 403, and 404.

PURPOSE(S) OF THE SYSTEM:

1. To provide online registration with single sign-on services for customers.

2. To facilitate online registration, provide enrollment capability, and administer internet-based services or features.

3. To maintain current and up-to-date address information to assure accurate and reliable delivery and fulfillment of postal products, services, and other material.

4. To obtain accurate contact information in order to deliver requested products, services, and other material.

5. To authenticate customer logon information for *usps.com*.

6. To permit customer feedback in order to improve *usps.com* or USPS products and services.

7. To enhance understanding and fulfillment of customer needs.

8. To verify a customer's identity when the customer establishes or attempts to access his or her account.

9. To identify, prevent, and mitigate the effects of fraudulent transactions.

10. To enhance the customer experience by improving the security of Change of Address (COA) and Hold Mail processes.

11. To protect USPS customers from becoming potential victims of mail fraud and identity theft.

12. To identify and mitigate potential fraud in the COA and Hold Mail processes.

13. To verify a customer's identity when applying for COA and Hold Mail services.

14. To provide online registration for Informed Address platform service for customers.

15. To authenticate customer logon information for Informed Address platform services.

16. To verify the name and address of the sender or the authority of the sender's representative when submitting an online International inquiry for a lost or damaged package on *usps.com,* such as the use of the International Assistant tool.

17. To link *usps.com* customer accounts with authorized third-party vendor accounts that allow customers to purchase postage and/or fees and print labels for USPS shipping and mailing services.

18. To facilitate the transmission of customer shipping information from third-party vendors to Click-n-Ship®.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Customers who register via the USPS website at *usps.com*.

CATEGORIES OF RECORDS IN THE SYSTEM:

1. Customer information: Name; customer ID(s); company name; job title and role; home, business, and billing address; phone number(s) and fax number; email(s); URL; text message number(s) and carrier; Automated Clearing House (ACH) information, Employer Identification Number (EIN), and account-linking identifier.

2. Identity verification information: Question, answer, username, user ID, password, email address, text message address and carrier, Employer Identification Number (EIN), and results of identity proofing validation.

3. Business specific information: Business type and location, business IDs, annual revenue, number of employees, industry, nonprofit rate status, mail owner, mail service provider, PC postage user, PC postage vendor, product usage information, annual and/or monthly shipping budget, payment method and information, planned use of product, age of website, and information submitted by, or collected from, business customers in connection with promotional marketing campaigns.

4. Customer preferences: Preferences to receive USPS marketing information, preferences to receive marketing information from USPS partners, preferred means of contact, preferred email language and format, preferred on-screen viewing language, product and/or service marketing preference.

5. Customer feedback: Method of referral to website.

6. Registration information: Date of registration.

7. Online user information: internet Protocol (IP) address, domain name, operating system versions, browser version, date and time of connection, Media Access Control (MAC) address, device identifier, information about the software acting on behalf of the user (*i.e.,* user agent), and geographic location.

8. International Inquiries: Name and address in Customer Registration account profile used to match with Sender name and address or Sender's representative authority to file an international inquiry for a lost or damaged package.

9. Click-n-Ship Account Linking Information: Customer Address Details, Authentication, Customer Contact Name, Currency, Label Metadata, Marketplace Label data, Order ID, Order Status, Shipping Code, Value, IP Address, MAC Address, Device Type, Browser Type, OAuth accessToken, OAuth expiry, OAuth refreshToken, OAuth refreshTokenExpiry, OAuth tokenType, Marketplace Data ID, Marketplace Data Version, Marketplace Data Account Type, Marketplace Data Account Identifier, Marketplace Data Reference ID, Marketplace Data Labels.

RECORD SOURCE CATEGORIES:

Customers, Individual Sender and Sender's representative filing an international inquiry for lost or damaged packages.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

Standard routine uses 1. through 7., 10., and 11. apply.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Automated database, computer storage media, and paper.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

By customer name, customer ID(s), phone number, mail, email address, IP address, text message address, and any customer information or online user information.

By tracking number for International package shipments for which an individual sender or sender's representative is filing an online International inquiry for loss or damage.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

1. ACH records are retained up to 2 years.

2. Records stored in the registration database are retained until the customer cancels the profile record, 3 years after the customer last accesses records, or until the relationship ends.

3. For small business registration, records are retained 5 years after the relationship ends.

4. Online user information may be retained for 6 months.

Records existing on paper are destroyed by burning, pulping, or shredding. Records existing on computer storage media are destroyed according to the applicable USPS media sanitization practice.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Paper records, computers, and computer storage media are located in controlled-access areas under supervision of program personnel. Access to these areas is limited to authorized personnel, who must be identified with a badge.

Access to records is limited to individuals whose official duties require such access. Contractors and licensees are subject to contract controls and unannounced on-site audits and inspections. Computers are protected by mechanical locks, card key systems, or other physical access control methods. The use of computer systems is regulated with installed security software, computer logon identifications, and operating system controls including access controls, terminal and transaction logging, and file management software. Online data transmissions are protected by encryption.

For small business registration, computer storage tapes and disks are maintained in controlled-access areas or under general scrutiny of program personnel. Access is controlled by logon ID and password as authorized by the Marketing organization via secure website. Online data transmissions are protected by encryption.

RECORD ACCESS PROCEDURES:

Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.5.

CONTESTING RECORD PROCEDURES:

See Notification Procedures and Record Access Procedures.

NOTIFICATION PROCEDURES:

Customers wanting to know if information about them is maintained in this system of records must address inquiries in writing to the system manager. Inquiries must contain name, address, and other identifying information.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

March 8, 2023, 88 FR 14400; December 27, 2018, 83 FR 66768; August 25, 2016, 81 FR 58542; June 30, 2016, 81 FR 42760; June 20, 2014, 79 FR 35389; January 23, 2014, 79 FR 3881; July 11, 2012, 77 FR 40921; October 24, 2011, 76 FR 65756; May 08, 2008, 73 FR 26155; April 29, 2005, 70 FR 22516.

SYSTEM NAME AND NUMBER:

USPS 860.000 Financial Transactions.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

USPS Headquarters; Integrated Business Solutions Services Centers;

Accounting Service Centers; Bank Secrecy Act (BSA) Anti-Money Laundering (AML) Compliance group; and contractor sites.

SYSTEM MANAGER(S):

Chief Financial Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

39 U.S.C. 401, 403, and 404; 31 U.S.C. 5318, 5325, 5331, and 7701.

PURPOSE(S) OF THE SYSTEM:

1. To provide financial products and services.

2. To respond to inquiries and claims related to financial products and services.

3. To fulfill requirements of BSA, AML statutes and regulations and Office of Foreign Assets Control (OFAC).

4. To support investigations related to law enforcement for fraudulent financial transactions.

5. To provide additional verification procedures to combat fraudulent financial transactions.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Customers who use online payment or funds transfer services.

2. Customers who file claims or make inquiries related to online payment services, funds transfers, money orders, and stored-value cards.

3. Customers who purchase financial instruments in an amount of $3000 or more per day. Financial instruments are limited to money orders, gift cards and international wire transfer service.

4. Customers who purchase or redeem financial instruments in a manner requiring collection of information as potential suspicious activities under anti-money laundering requirements.

5. Beneficiaries from financial instruments totaling more than $10,000 in 1 day.

6. Specially Designated Nationals and Blocked Persons List (SDNs) as defined and mandated by the OFAC.

CATEGORIES OF RECORDS IN THE SYSTEM:

1. Customer information: Name, customer ID(s), mail and email address, telephone number, occupation, type of business, Employer Identification Number (EIN), and customer history.

2. Identity verification information: Date of birth, username and/or ID, password, Social Security Number (SSN) or tax ID number, and driver's license number (or other type of ID if driver's license is not available, such as Alien Registration Number, Passport Number, Military ID, Tax ID Number). (Note: For online payment services, SSNs are collected, but not retained, in order to verify ID.)

3. Billers registered for online payment services: Biller name and contact information, bill detail, and bill summaries.

4. Transaction information: Name, address, and phone number of purchaser, payee, and biller; amount, date, and location; credit and/or debit card number, type, and expiration; sales, refunds, and fees; type of service selected and status; sender and recipient bank account and routing number; bill detail and summaries; transaction number, serial number, and/or reference number or other identifying number, pay out agent name and address; type of payment, currency, and exchange rate; Post Office information such as location, phone number, and terminal; employee ID numbers, license number and state, and employee comments.

5. Information to determine credit-worthiness: Period at current residence, previous address, and period of time with same phone number.

6. Information related to claims and inquiries: Name, address, phone number, signature, SSN, location where product was purchased, date of issue, amount, serial number, and claim number.

7. Online user information: internet Protocol (IP) address, domain name, operating system version, browser version, date and time of connection, and geographic location.

8. Funds Transaction Report (FTR) Postal Service (PS) Form 8105–A:

a. Type of Transaction (completed by customer): on behalf of self, on behalf of another individual, on behalf of a business/organization, law enforcement agent or government representative on behalf of an agency, private courier on behalf of individual, private courier on behalf of a business/organization, armored car service on behalf of a business/individual.

b. Customer Information (completed by customer): last name/first name, address (number, street, box, suite/apt no.), city, state, ZIP CodeTM, country, date of birth (MM/DD/YYYY), SSN, telephone number (include area code); Photo ID: driver's license no. (U.S. only—must indicate state), resident alien/permanent resident ID no., other ID (U.S./state government-issued IDs, including tribal, and Mexican matricular consular), state ID no. (U.S. only—must indicate state), military ID no. (U.S. only), passport no. (must indicate country); Describe other ID: ID number, issuing state, issuing country (passport), occupation (be as specific as possible); (Completed by Postal ServiceTM employee): round date stamp.

c. Other Person/Business/Organization on Whose Behalf Transaction Is Being Conducted (completed by customer): last name/first name or business name or organization name (no acronyms), SSN or employer ID number (EIN), North American Industry Classification System (NAICS) (if business), type of business/organization/occupation, address (number, street, box, suite/apt no.), city, state, ZIP CodeTM, country, date of birth (MM/DD/YYYY), telephone number (include area code), ID type, ID number, issuing state;

d. Completed by Postal Service TMEmployee: type of transaction (check one)—purchased ($3,000.00 or more) or redeemed/cashed (over $10,000.00), total face value (excluding fee), transaction date (MM/DD/YYYY), beginning serial no. thru ending serial no. money order ranges 1–2, number of money orders sold, number of money orders redeemed/cashed, number of gift cards sold (provide numbers in section on back of form), funds transfer 1 Sure MoneyTM/Dinero Seguro, signature of USPS® employee, Post OfficeTM ZIP CodeTM;

e. Law Enforcement Agent of Government Representative on Behalf of an Agency (completed by customer): last name/first name, date of birth (MM/DD/YYYY), work telephone number (include area code), law enforcement agent/government representative photo ID number (if photo ID does not have a number please use agent/representative driver's license number), type of ID: law enforcement ID, government representative ID, driver's license number (must note state if using driver's license), state, agency name (no acronyms), address (number, street, box, suite/apt. no.), city, state, ZIP CodeTM, occupation, agency EIN, NAICS;

f. Armored Car Service Information (completed by customer): armored car business name (no acronyms), EIN, telephone number (include area code), address (number, street, box, suite/apt no.), city, state, ZIP CodeTM; and

g. Completed by Postal Service Employee (Continued): type of transaction (check one)—purchased ($3,000.00 or more) or redeemed/cashed (over $10,000.00), additional transaction numbers for money orders, funds transfer Sure MoneyTM/Dinero Seguro, and gift cards—beginning serial no. thru ending serial no. money order ranges 3–6, Sure MoneyTM/Dinero Seguro 2–5, and gift card numbers 1–4.

9. Suspicious Transaction Report (STR) PS Form 8105–B (completed by Postal ServiceTMemployee): activity

type—purchased, redeemed/cashed, other (describe in comments section), begin serial no. thru end serial no. money order ranges 1–3, transaction amount, transaction date, transaction time, recorded by camera, check box if a debit/credit card was used in the transaction (do not include any information from the debit/credit card on this form), description of customer(s) 1–4—sex (M/F), approximate age, height, weight, ethnicity, round date stamp, Post OfficeTM ZIP CodeTM, comments (check all that apply), vehicle description (if available)—make, type, color, license number, license state, comments, money order ranges 4–5, gift cards 1–2, funds transfer Sure Money®/ Dinero Seguro® 1–2, business name/ customer last name, first name, address (number, street, box, suite/apt. no.), city, state, ZIP CodeTM, country, type of business, date of birth (MM/DD/YYYY), SSN, driver's license no., state, other ID no., type of other ID, mailpiece information (if available)—mailpiece number, mailpiece type, additional comments.

RECORD SOURCE CATEGORIES:

Customers, recipients, financial institutions, and USPS employees.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Standard routine uses 1. through 7., 10., and 11. apply. In addition;

a. Legally required disclosures to agencies for law enforcement purposes include disclosures of information relating to money orders, funds transfers, and stored-value cards as required by BSA, OFAC and anti-money laundering statutes, regulations and requirements.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Automated database, computer storage media, microfiche, and paper.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

For online payment and funds transfer services, information is retrieved by customer name, customer ID(s), transaction number, or address.

Claim information is retrieved by name of purchaser or payee, claim number, serial number, transaction number, check number, customer ID(s), or ZIP Code.

Information related to BSA, OFAC and AML is retrieved by customer name; SSN; alien registration, passport, or driver's license number; serial number; transaction number; ZIP Code; transaction date; data entry operator number; and employee comments, and individuals that appear on the Specially Designated Nationals and Blocked Persons List (SDNs) as defined and mandated by the OFAC.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

1. Summary records, including bill due date, bill amount, biller information, biller representation of account number, and the various status indicators, are retained 2 years from the date of processing.

2. For funds transfers, transaction records are retained 3 years.

3. Records related to claims are retained up to 3 years from date of final action on the claim.

4. Forms related to fulfillment of BSA, anti-money laundering requirements are retained for a 5-year and one-month period.

5. Related automated records are retained the same 5-year and one-month period and purged from the system quarterly after the date of creation.

6. Enrollment records related to online payment services are retained 7 years after the subscriber's account ceases to be active or the service is cancelled.

7. Account banking records, including payment history, Demand Deposit Account (DDA) number, and routing number, are retained 7 years from the date of processing.

8. Online user information may be retained for 6 months.

Records existing on paper are destroyed by burning, pulping, or shredding. Records existing on computer storage media are destroyed according to the applicable USPS media sanitization practice.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Paper records, computers, and computer storage media are located in controlled-access areas under supervision of program personnel. Access to these areas is limited to authorized personnel, who must be identified with a badge.

Access to records is limited to individuals whose official duties require such access. Contractors and licensees are subject to contract controls and unannounced on-site audits and inspections. Computers are protected by mechanical locks, card key systems, or other physical access control methods. The use of computer systems is regulated with installed security software, computer logon identifications, and operating system controls including access controls, terminal and transaction logging, and file management software. Online data transmissions are protected by encryption.

RECORD ACCESS PROCEDURES:

Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.5.

CONTESTING RECORD PROCEDURES:

See Notification Procedure below and Record Access Procedures above.

NOTIFICATION PROCEDURES:

For online payment services, funds transfers, and stored-value cards, individuals wanting to know if information about them is maintained in this system must address inquiries in writing to the Chief Marketing Officer and Executive Vice President. Inquiries must contain name, address, and other identifying information, as well as the transaction number for funds transfers.

For money order claims, or BSA, OFAC and anti-money laundering documentation, inquiries should be addressed to the Chief Financial Officer and Executive Vice President. Inquiries must include name, address, or other identifying information of the purchaser (such as driver's license, Alien Registration Number, Passport Number, etc.), and serial or transaction number. Information collected for anti-money laundering purposes will only be provided in accordance with Federal BSA, OFAC, anti-money laundering laws, regulations and requirements.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Systems Exempted From Certain Provisions of the Act:

USPS has established regulations at 39 CFR 266.9 that exempt information contained in this system of records from various provisions of the Privacy Act in order to conform to the prohibition in the Bank Secrecy Act, 31 U.S.C. 5318(g)(2), against notification of the individual that a suspicious transaction has been reported.

HISTORY:

May 8, 2008, 73 FR 26155; April 29, 2005, 70 FR 22516.

SYSTEM NAME AND NUMBER:

USPS 910.000, Identity and Document Verification Services.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

USPS Marketing, Headquarters; Integrated Business Solutions Services Centers; and contractor sites.

SYSTEM MANAGER(S):

Chief Information Officer and Executive Vice President, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260–1500.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

39 U.S.C. 401, 403, 404, and 411.

PURPOSE(S) OF THE SYSTEM:

1. To provide services related to identity and document verification services.

2. To issue and manage public key certificates, user registration, email addresses, and/or electronic postmarks.

3. To provide secure mailing services.

4. To protect business and personal communications.

5. To enhance personal identity and privacy protections.

6. To improve the customer experience and facilitate the provision of accurate and reliable delivery information.

7. To identify, prevent, or mitigate the effects of fraudulent transactions.

8. To support other Federal Government Agencies by providing authorized services.

9. To ensure the quality and integrity of records.

10. To enhance the customer experience by improving the security of Change-of-Address (COA) and Hold Mail processes, along with other products, services and features that require identity proofing and document verification.

11. To protect USPS customers from becoming potential victims of mail fraud and identity theft.

12. To identify and mitigate potential fraud in the COA and Hold Mail processes, along with other products, services and features that require identity proofing and document verification.

13. To verify a customer's identity when applying for COA and Hold Mail services, along with other products, services and features that require identity proofing and document verification.

14. To provide an audit trail for COA and Hold Mail requests (linked to the identity of the submitter).

15. To enhance remote identity proofing with a Phone Verification and One-Time Passcode solution.

16. To enhance remote identity proofing, improve fraud detection and customer's ability to complete identity proofing online with a Device Reputation Remote Identity Verification solution.

17. To verify a customer's Identity using methods and Identity Proofing standards that voluntarily align with NIST Special Publication 800.63 and support other Federal Agency partner security requirements.

18. To enhance In-Person identity proofing, improve Identity Document fraud detection and enable a customer to successfully complete identity proofing activities required for access to Postal Service products, services and features.

19. To enhance In-Person identity proofing, improve Identity Document fraud detection and enable a customer to successfully complete identity proofing activities as required by partnering Federal Agencies to authorize or allow individual customer access to a privilege, system, or role.

20. To facilitate the In-Person enrollment process for the Informed Delivery® feature.

21. To provide customers with the option to voluntarily scan the barcode on the back of government issued IDs to capture name and address information that will be used to confirm eligibility and prefill information collected during the In-Person Informed Delivery enrollment process.

22. To provide identity verification documents to United States government agencies and third parties, with customer consent, for validation and security.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Customers who apply for identity and document verification services.

2. Customers who may require identity verification for Postal products, services and features.

3. USPS customers who sign-up, register or enroll to participate as users in programs, request features, or obtain products and/or services that require document or identity verification.

4. Individual applicants and users that require identity verification or document verification services furnished by the Postal Service in cooperation with other Government agencies.

CATEGORIES OF RECORDS IN THE SYSTEM:

1. Customer information: Name, address, customer ID(s), telephone number, text message number and carrier, mail and email address, date of birth, place of birth, company name, title, role, Employer Identification Number (EIN), and employment status.

2. Customer preference information: Preferred means of contact.

3. Authorized User Information: Names and contact information of users who are authorized to have access to data.

4. Verification and payment information: Credit or debit card information or other account number, government issued ID type and number, verification question and answer, and payment confirmation code. (Note: Social Security Number and credit or debit card information may be collected, but not stored, in order to verify ID.)

5. Biometric information: Fingerprint, photograph, height, weight, and iris scans. (Note: Information may be collected, secured, and returned to customer or third parties at the request of the customer, but not stored.)

6. Digital certificate information: Customer's public key(s), certificate serial numbers, distinguished name, effective dates of authorized certificates, certificate algorithm, date of revocation or expiration of certificate, and USPS-authorized digital signature.

7. Online user information: Device identification, device reputation risk and confidence scores.

8. Transaction information: Clerk signature; transaction type, date and time, location, source of transaction; product use and inquiries; Change of Address (COA) and Hold Mail transactional data.

9. Electronic information: Information related to encrypted or hashed documents.

10. Recipient information: Electronic signature ID, electronic signature image, electronic signature expiration date, and timestamp.

11. In-Person Proofing and Enhanced Identity Verification Attributes: Contents of Valid Identification (ID) Documents; High resolution images of front and back of ID documents, bar code on ID Document and the content of displayed and encoded fields on ID documents that may be collected and stored in order to facilitate security validation and Identity Proofing of an applicant, participant or customer's ID; Facial Image; Name, Address, and Unique ID Document number; Birthdate, Eye Color, Height and Weight; Signature; Organ donation preference.

12. Strong ID Documents used for In-Person Identity Proofing: Photo ID, unique ID Number and the name of the Individual being identified; Passports, Passport cards; State ID Cards, State Driver's Licenses: Uniformed Service ID's, and Government ID documents.

13. Fair ID Documents used for In-Person Identity Proofing: Residential Lease, Real Estate Deed of Trust, Voter Registration Card, Vehicle Registration Card, Home Insurance Policy Documents, Vehicle Insurance Policy Documents.

RECORD SOURCE CATEGORIES:

Individual Customers, Users, Participants and Applicants.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

Standard routine uses 1. through 7., 10., and 11. apply.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Automated databases, computer storage media, and paper.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

By customer name, customer ID(s), distinguished name, certificate serial number, receipt number, transaction date, and email addresses.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

1. Records related to Pending Public Key Certificate Application Files are added as received to an electronic database, moved to the authorized certificate file when they are updated with the required data, and records not updated within 90 days from the date of receipt are destroyed.
2. Records related to the Public Key Certificate Directory are retained in an electronic database, are consistently updated, and records are destroyed as they are superseded or deleted.
3. Records related to the Authorized Public Key Certificate Master File are retained in an electronic database for the life of the authorized certificate.
4. When the certificate is revoked, it is moved to the certificate revocation file.
5. The Public Key Certificate Revocation List is cut off at the end of each calendar year and records are retained 30 years from the date of cutoff. Records may be retained longer with customer consent or request.
6. Other records in this system are retained 7 years, unless retained longer by request of the customer.
7. Records related to electronic signatures are retained in an electronic database for 3 years.
8. Other categories of records are retained for a period of up to 30 days.
9. Driver's License data will be retained for 5 years.
10. COA and Hold Mail transactional data will be retained for 5 years.
11. Records related to Phone Verification/One-Time Passcode and Device Reputation assessment will be retained for 7 years.
12. Records collected for Identity Proofing at the Identity Assurance Level 2 (IAL–2), including ID document images, Identity Verification Attributes, and associated data will be retained up to 5 years, or as stipulated within Interagency Agreements (IAAs) with partnering Federal Agencies.

Records existing on paper are destroyed by burning, pulping, or shredding. Records existing on computer storage media are destroyed according to the applicable USPS media sanitization practice.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Paper records, computers, and computer storage media are located in controlled-access areas under supervision of program personnel. Access to these areas is limited to authorized personnel, who must be identified with a badge.

Access to records is limited to individuals who need the information to perform their job and whose official duties require such access.

Contractors and licensees are subject to contract controls and unannounced on-site audits and inspections.

Computers are protected by mechanical locks, card key systems, or other physical access control methods. The use of computer systems is regulated with installed security software, computer logon identifications, and operating system controls including access controls, terminal and transaction logging, and file management software.

Key pairs are protected against cryptanalysis by encrypting the private key and by using a shared secret algorithm to protect the encryption key, and the certificate authority key is stored in a separate, tamperproof, hardware device. Activities are audited, and archived information is protected from corruption, deletion, and modification.

For authentication services and electronic postmark, electronic data is transmitted via secure socket layer (SSL) encryption to a secured data center. Computer media are stored within a secured, locked room within the facility. Access to the database is limited to the system administrator, database administrator, and designated support personnel. Paper forms are stored within a secured area within locked cabinets.

RECORD ACCESS PROCEDURES:

Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.5.

CONTESTING RECORD PROCEDURES:

See Notification Procedure and Record Access Procedures above.

NOTIFICATION PROCEDURES:

Customers wanting to know if other information about them is maintained in this system of records must address inquiries in writing to the system manager. Inquiries must contain name, address, email, and other identifying information.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

December 15, 2021; 86 FR 71294; March 16, 2020, 85 FR 14982; December 13, 2018, 83 FR 64164; December 22, 2017, 82 FR 60776; August 29, 2014, 79 FR 51627; October 24, 2011, 76 FR 65756; April 29, 2005, 70 FR 22516.

Christopher Doyle,

Attorney, Ethics & Legal Compliance.

[FR Doc. 2024–16505 Filed 7–25–24; 8:45 am]

BILLING CODE 7710–12–P

SECURITIES AND EXCHANGE COMMISSION

[SEC File No. 270–346, OMB Control No. 3235–0392]

Submission for OMB Review; Comment Request; Extension: Rule 15g–3

Upon Written Request, Copies Available From: Securities and Exchange Commission, Office of FOIA Services, 100 F Street NE, Washington, DC 20549–2736

Notice is hereby given that pursuant to the Paperwork Reduction Act of 1995 (''PRA'') (44 U.S.C. 3501 *et seq.*), the Securities and Exchange Commission (''Commission'') has submitted to the Office of Management and Budget (''OMB'') a request for approval of extension of the existing collection of information provided for in Rule 15g–3—Broker or dealer disclosure of quotations and other information relating to the penny stock market (17 CFR 240.15g–3) under the Securities Exchange Act of 1934 (15 U.S.C. 78a *et seq.*).

Rule 15g–3 requires that brokers and dealers disclose to customers current quotation prices or similar market information in connection with transactions in penny stocks. The purpose of the rule is to increase the level of disclosure to investors concerning penny stocks generally and specific penny stock transactions.

The Commission estimates that approximately 170 broker-dealers will each spend an average of approximately 87.0833333 hours annually to comply with this rule. Thus, the total time