This document is scheduled to be published in the Federal Register on 03/16/2020 and available online at **federalregister.gov/d/2020-05232**, and on **govinfo.gov**

POSTAL SERVICE

Privacy Act; Notice of a modified 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 a Customer Privacy Act Systems of Records (SOR). These changes are being made to support ongoing efforts to identify, mitigate and prevent fraudulent transactions.

DATES: These revisions will become effective without further notice on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER], unless comments received on or before that date result in a contrary determination.

ADDRESSES: Comments may be mailed or delivered to the Privacy and Records Management Office, United States Postal Service, 475 L'Enfant Plaza SW, Room 1P830, Washington, DC 20260-1101. Copies of all written comments will be available at this address for public inspection and photocopying between 8 a.m. and 4 p.m., Monday through Friday.

FOR FURTHER INFORMATION CONTACT: Janine Castorina, Chief Privacy and Records Management Officer, Privacy and Records Management Office, 202-268-3069 or *privacy@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 Systems of Records, USPS 910.000 Identity and Document Verification Services, should be revised to support efforts to enhance remote identity proofing capabilities and improve the customer's ability to successfully complete required online identity proofing activities.

The Postal Service is implementing Device Reputation assessment technology to enhance its existing remote identity proofing solution, and to detect to the best extent possible, fraudulent history and characteristics of a malicious user. The Postal Service's objective in implementing the Device Reputation solution is to assess the risk associated with a user and establish a confidence level for that assessment. The validation and verification of the minimum attributes necessary is used to accomplish identity proofing.

Device Reputation uses the unique characteristics of a user's electronic device profile to complete identity verification and make a recommendation on the risk level of the user. Devices are profiled during the verification process and compared to a digital identity, generated from device profiles and activity collected across industry. Based on the past activity of that digital identity, as well as a number of attributes associated with the device itself, fraud risk and confidence scores are generated for that identity verification transaction. The device risk score expresses the fraud risk level of the transaction, while the confidence score establishes the level of confidence in the digital identity match. Digital identity represents the online footprint of the user. USPS Identity Verification Services (IVS) will use those risk and confidence scores to assess and make decisions about granting users access to USPS products, services and features. The scores will be saved by IVS to support post-transaction fraud analysis efforts and to respond to individual records requests consistent with Privacy Act requirements.

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 has been sent to Congress and to the

Office of Management and Budget for their evaluations. The Postal Service does not expect this amended systems of records to have any adverse effect on individual privacy rights. The notice for

USPS 910.000, Identity and Document Verification

Services, provided below in its entirety, is as follows:

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; (202) 268-6900.

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.

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 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.

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 and services.

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. Individuals 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, 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.

RECORD SOURCE CATEGORIES:

Customers and Users

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 OF 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.

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.

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 13, 2018, 83 FR 64164; December 22, 2017, *82 FR 60776;*

August 29, 2014, 79 FR 51627; October 24, 2011, 76 FR 65756

* * * * *

Joshua J. Hofer,

Attorney, Federal Compliance.

[FR Doc. 2020-05232 Filed: 3/13/2020 8:45 am; Publication Date: 3/16/2020]