POSTAL SERVICE

Privacy Act of 1974; System of Records

AGENCY: Postal Service™.

ACTION: Notice of a modified systems of records.

SUMMARY: The United States Postal Service® (Postal Service) is proposing to revise five Customer Privacy Act Systems of Records (SORs). These changes are being made to support the new Address Matching Database, which will be used to identify, prevent, and mitigate fraudulent activity within the Change of Address and Hold Mail processes.

DATES: These revisions will become effective without further notice on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*], unless, in response to comments received on or before that date, the Postal Service makes any substantive change to the purpose or routine uses set forth, or to expand the availability of information in this system, as described in this notice. If the Postal Service determines that certain portions of this SOR should not be implemented, or that implementation of certain portions should be postponed in light of comments received, the Postal Service may choose to implement the remaining portions of the SOR on the stated effective date, and will provide notice of that action.

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 following Postal Service Privacy Act System of Records are being revised to facilitate the new

Address Matching Database for the purposes of protecting the mail and detecting fraudulent activity within the Change of Address and Hold Mail processes:

- USPS 800.000 Address Change, Mail Forwarding, and Related Services
- USPS 810.100 www.usps.com Registration
- USPS 810.200 www.usps.com Ordering, Payment and Fulfillment
- USPS 820.200 Mail Management and Tracking Activity
- USPS 820.300 Informed Delivery

In an effort to provide secure mailing services, the Postal Service is using a new Address Matching Database to identify, prevent, and mitigate fraudulent activity within the Change of Address and Hold Mail processes. The Postal Service is establishing a dataflow between existing customer systems and the Address Matching Database. This dataflow will allow the Address Matching Database to: confirm if there is an address match when a new Hold Mail request is submitted; confirm the presence of a Change of Address request when a Hold Mail request is submitted during a 30 day time frame; and confirm the presence of a Hold Mail request when a Change of Address request is submitted during a 30 day time frame. The Address Matching Database will also send confirmation notifications to customers who submit a Hold Mail request.

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 these amended systems of records to have any adverse effect on individual privacy rights. The affected systems are as follows:

SYSTEM NAME AND NUMBER:
USPS 800.000, Address Change, Mail Forwarding, and Related Services.

SYSTEM CLASSIFICATION:
None.

SYSTEM LOCATION:
USPS National Customer Support Center (NCSC), Computerized Forwarding System (CFS) sites, Post Offices, USPS Processing and Distribution Centers, USPS IT Eagan Host Computing Services Center, and contractor sites.

SYSTEM MANAGER(S)
Vice President, Enterprise Analytics, United States Postal Service, 475 L'Enfant Plaza, SW, Washington, DC 20260-5626, (202) 268-7542.
Vice President, Delivery Operations, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260-7116, (202) 268-6500.
Vice President, Customer Experience, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260-0004, (202) 268-2252.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
39 U.S.C. 401(2), 403, and 404(a)(1).

PURPOSE(S) OF THE SYSTEM:
1. To provide mail forwarding and COA services, including local community information, and move related advertisements.
2. To provide address correction services.
3. To counter efforts to abuse the COA process.
4. To provide address information to the American Red Cross or other disaster relief organization about a customer who has been relocated because of disaster.
5. To support investigations related to law enforcement for fraudulent transactions.
6. To provide automatic updates to USPS customer systems using mail forwarding and COA services.
7. To facilitate communication between USPS customers and the Postal Service with regard to COA and address correction services.
8. To enhance the customer experience by improving the security of COA and Hold Mail processes.
9. To protect USPS customers from becoming potential victims of mail fraud and identity theft.
10. To identify and mitigate potential fraud in the COA and Hold Mail processes.
11. To verify a customer's identity when applying for COA and Hold Mail services.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
Customers requesting Change of Address (COA), mail forwarding, or other related services either electronically or in writing.
Customers who are victims of a natural disaster who request mail forwarding services through the Postal Service or the American Red Cross.

CATEGORIES OF RECORDS IN THE SYSTEM:
1. *Customer information:* Name, title, signature, customer number, old address, new address, filing date, email address(es), telephone numbers, and other contact information.
2. *Verification and payment information:* Credit and/or debit card number, type, and expiration date; or date of birth and driver's state and license number; information for identity verification; and billing information. Customers who are victims of a natural disaster who request mail forwarding service electronically may be required to provide date of birth for verification if credit and/or debit card information is unavailable.
3. *Demographic information:* Designation as individual/family/business.

4. *Customer preferences:* Permanent or temporary move; mail forwarding instructions; service requests and responses.
5. *Customer inquiries and comments:* Description of service requests and responses.
6. *Records from service providers* for identity verification.
7. *Online user information:* Internet Protocol (IP) address, domain name, operating system versions, browser version, date and time of connection, and geographic location.
8. *Protective Orders.*

RECORD SOURCE CATEGORIES:
Customers, personnel, contractors, service providers, and for call center operations, commercially available sources of names, addresses, and telephone numbers. For emergency change-of-addresses only, commercially available sources of names, previous addresses, and dates of birth. For alternative authentication, sources of names, previous and new addresses, dates of birth, and driver's state and license number.

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. In addition:

a. *Disclosure upon request.* The new address of a specific business or organization that has filed a permanent change-of-address order may be furnished to any individual on request. (Note: The new address of an individual or family will not be furnished pursuant to this routine use, unless authorized by one of the standard routine uses listed above or one of the specific routine uses listed below.) If a domestic violence shelter has filed a letter on official letterhead from a domestic violence coalition stating (i) that such domestic violence coalition meets the requirements of 42 U.S.C. § 10410 and (ii) that the organization filing the change of address is a domestic violence shelter, the new address shall not be released except pursuant to routine use d, e, or f pursuant to the order of a court of competent jurisdiction.

b. *Disclosure for Address Correction.* Disclosure of any customer's new permanent address may be made to a mailer, only if the mailer is in possession of the name and old address: from the National Change-of-Address Linkage (NCOALink®) file if the mailer is seeking corrected addresses for a mailing list; from the Computerized Forwarding System (CFS), from the Postal Automated Redirection System (PARS) if a mailpiece is undeliverable as addressed, or from the Locatable Address Conversion System if an address designation has been changed or assigned. Copies of change-of-address orders may not be furnished. In the event of a disaster or manmade hazard, temporary address changes may be disclosed to a mailer when, in the sole determination of the Postal Service, such disclosure serves the primary interest of the customer, for example, to enable a mailer to send medicines directly to the customer's temporary address, and only if the mailer is in possession of the customer's name and permanent address. If a domestic violence shelter has filed a letter on official letterhead from a domestic violence coalition stating (i) that such domestic violence coalition meets the requirements of 42 U.S.C. § 10410 and (ii) that the organization filing the change of address is a domestic violence shelter, the new address shall not be released except pursuant to routine use d, e, or f pursuant to the order of a court of competent jurisdiction.

c. *Disclosure for Voter Registration.* Any customer's permanent change of address may be disclosed to a duly formed election board or registration commission using permanent voter registration. Copies of change of address orders may be furnished.

d. *Disclosure to Government Agency.* Any customer's permanent or temporary change of address information may be disclosed to a federal, state, or local government agency upon prior written certification that the information is required for the performance of its duties. A copy of the change of address order may be furnished. Name and address information may be disclosed to government planning authorities, or firms under contract with those authorities, if an address designation has been changed or assigned.

e. *Disclosure to Law Enforcement Agency.* Any customer's permanent or temporary change

of address information may be disclosed to a law enforcement agency, for oral requests made through the Postal Inspection Service, but only after the Postal Inspection Service has confirmed that the information is needed for a criminal investigation. A copy of the change of address order may be furnished.

f. *Disclosure for Service of Process.* Any customer's permanent or temporary change of address information may be disclosed to a person empowered by law to serve legal process, or the attorney for a party in whose behalf service will be made, or a party who is acting pro se, upon receipt of written information that meets prescribed certification requirements. Disclosure will be limited to the address of the specifically identified individual (not other family members or individuals whose names may also appear on the change of address order). A copy of the change of address order may not be furnished.

g. *Disclosure for Jury Service.* Any customer's change of address information may be disclosed to a jury commission or other court official, such as a judge or court clerk, for purpose of jury service. A copy of the change of address order may be furnished.

h. *Disclosure at Customer's Request.* If the customer elects, change of address information may be disclosed to government agencies or other entities.

i. *Disclosure to a disaster relief organization.* Any customer's permanent or temporary change of address may be disclosed to the American Red Cross or other disaster relief organizations, if that address has been impacted by disaster or manmade hazard.

All routine uses are subject to the following exception: Information concerning an individual who has filed an appropriate protective court order with the postmaster/CFS manager will not be disclosed under any routine use except pursuant to the order of a court of competent jurisdiction.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:
Records are retrieved by the following methods: For paper records: by name, address, date, and ZIP Code. For electronic records: by name, address, date, ZIP Code™, and customer number for electronic change of address and related service records; by name, address, and email address for customer service records.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:
1. National change-of-address and mail forwarding records are retained 4 years from the effective date.
2. Delivery units access COA records from the Change- Of-Address Reporting System (COARS) database, which retains 2 years of information from the COA effective date. The physical change-of-address order is retained in the CFS unit for 30 days if it was scanned, or 18 months if it was manually entered into the national database.
3. Online user information may be retained for 12 months. Records existing on paper are destroyed by 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.

RECORD ACCESS PROCEDURES:
Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act.

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 should address inquiries to their local postmaster. Inquiries should contain full name, address, effective date of change order, route number (if known), and ZIP Code. Customers wanting to know if information about them is also maintained in the NCOA File should address such inquiries to: Manager, NCOA, National Customer Support Center, United States Postal Service, 6060 Primacy Parkway, Memphis, TN 38188.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:
None.

HISTORY:
June 30, 2016, 81 FR 42760; August 21, 2014, 79 FR 49543; September 13, 2012, 77 FR 56676; July 17, 2008, 73 FR 41135; April 29, 2005, 70 FR 22516.

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.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
Customers who register via the USPS Web site at *usps.com*.

CATEGORIES OF RECORDS COVERED BY 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; and Automated Clearing House (ACH) information.
2. *Identity verification information:* Question, answer, username, user ID, password, email address, text message address and carrier, 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 Web site.
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.

RECORD SOURCE CATEGORIES:
Customers.

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.

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 Web site. 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 266.6.

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:
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 810.200, www.usps.com Ordering, Payment, and Fulfillment.

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, 404, and 407; 13 U.S.C. 301–307; and 50 U.S.C. 1702.

PURPOSE(S) OF THE SYSTEM:
1. To fulfill orders for USPS products and services.
2. To promote increased use of the mail by providing electronic document preparation and mailing services for customers.
3. To provide shipping supplies and services, including return receipts and labels.
4. To provide recurring ordering and payment services for products and services.
5. To support investigations related to law enforcement for fraudulent financial transactions.
6. To satisfy reporting requirements for customs purposes.
7. To support the administration and enforcement of U.S. customs, export control, and export statistics laws.
8. To enhance the customer experience by improving the security of Change of Address (COA) and Hold Mail processes.
9. To protect USPS customers from becoming potential victims of mail fraud and identity theft.
10. To identify and mitigate potential fraud in the COA and Hold Mail processes.
11. To verify a customer's identity when applying for COA and Hold Mail services.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
Customers who place orders and/or make payment for USPS products and services through *usps.com*.

CATEGORIES OF RECORDS IN THE SYSTEM:
1. *Customer information:* Name, customer ID(s), phone and/or fax number, mail address, and email address.
2. *Payment information:* Credit and/or debit card number, type, and expiration date, billing information, ACH information.
3. *Shipping and transaction information:* Product and/or service ID numbers, descriptions, value, date, postage and fees, and prices; name and address(es) of recipients; order number and delivery status; electronic address lists; electronic documents or images; job number; and applicable citation or legend required by the foreign trade regulations.
4. Claims submitted for lost or damaged merchandise.
5. *Online user information:* Internet Protocol (IP) address, domain name, operating system version, browser version, date and time of connection, and geographic location.

RECORD SOURCE CATEGORIES:
Customers.

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. In addition:

a. Customs declaration records may be disclosed to domestic and foreign customs agencies and postal operators, as well as intermediary companies involved in electronic data exchanges, for the purpose of facilitating carriage, security protocols, foreign or domestic customs processing, payment to operators, or delivery.
b. Records may be disclosed to the Office of Foreign Assets Control, the Bureau of Industry and Security, Customs and Border Protection, and other government authorities for the purpose of administering and enforcing export control laws, rules, and policies, including 50 U.S.C. 1702.
c. Customs declaration records may be disclosed to the U.S. Census Bureau for export statistical purposes pursuant to 13 U.S.C. 301-307.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:
Automated databases, computer storage media, and digital and paper files.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:
By customer name, customer ID(s), phone number, mail or email address, or job number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

1. Records related to mailing online and online tracking and/or confirmation services supporting a customer order are retained for up to 30 days from completion of fulfillment of the order, unless retained longer by request of the customer.
2. Records related to shipping services and domestic and international labels are retained up to 90 days.
3. Delivery Confirmation and return receipt records are retained for 6 months.
4. Signature Confirmation records are retained for 1 year.
5. ACH records are retained for up to 2 years.
6. Customs declaration records stored in electronic data systems are retained 5 years, and then purged according to the requirement of domestic and foreign customs services. Other hard copy customs declaration records are retained 30 days.
7. Other records related to shipping services and domestic and international labels are retained up to 90 days.
8. Other customer records are retained for 3 years after the customer relationship ends.
9. Online user information may be retained for 12 months.

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 transmission is protected by encryption, dedicated lines, and authorized access codes. For shipping supplies, data is protected within a stand-alone system within a controlled-access facility.

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 266.6.

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, customer ID(s), and order number, if known.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:
None.

HISTORY:
May 24, 2017, 82 FR 23850; September 13, 2012, 77 FR 56676; June 27, 2012, 77 FR 38342; June 17, 2011, 76 FR 35483; May 12, 2009, 74 FR 22186; May 08, 2008, 73 FR 26155; May 06, 2005, 70 FR 24128; April 29, 2005, 70 FR 22516.

SYSTEM NAME AND NUMBER:
USPS 820.200, Mail Management and Tracking Activity.

SECURITY CLASSIFICATION:
None.

SYSTEM LOCATION:
USPS Headquarters; Integrated Business Solutions Services Centers; USPS IT Eagan Host Computing Services Center; and Mail Transportation Equipment Service Centers.

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.

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 mail acceptance, induction, and scheduling services.
2. To fulfill orders for mail transportation equipment.
3. To provide customers with information about the status of mailings within the USPS network or other carrier networks.
4. To provide customers with mail or package delivery options.
5. To provide business mailers with information about the status of mailings within the USPS mail processing network.
6. To help mailers identify performance issues regarding their mail.
7. To provide delivery units with information needed to fulfill requests for mail redelivery and hold mail service at the address and for the dates specified by the customer.
8. To enhance the customer experience by improving the security of Change of Address (COA) and Hold Mail processes.
9. To protect USPS customers from becoming potential victims of mail fraud and identity theft.
10. To identify and mitigate potential fraud in the COA and Hold Mail processes.
11. To verify a customer's identity when applying for COA and Hold Mail services.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
Customers who use USPS mail management and tracking services.

CATEGORIES OF RECORDS IN THE SYSTEM:
1. *Customer information:* Customer or contact name, mail and email address(es), title or role, phone number(s), text message number, and cell phone carrier.
2. *Identification information:* Customer ID(s), last four digits of Social Security Number (SSN), D-U-N-S Number; mailer and mailing ID, advertiser name/ID, username, and password.
3. *Data on mailings:* Paper and electronic data on mailings, including postage statement data (such as volume, class, rate, postage amount, date and time of delivery, mailpiece count), destination of mailing, delivery status, mailing problems, presort information, reply mailpiece information, container label numbers, package label, Special Services label, article number, and permit numbers.
4. *Payment information:* Credit and/or debit card number, type, and expiration date; ACH information.
5. *Customer preference data:* Hold mail begin and end date, redelivery date, delivery options, shipping and pickup preferences, drop ship codes, comments and instructions,

mailing frequency, preferred delivery dates, and preferred means of contact.
6. *Product usage information:* Special Services label and article number.
7. *Mail images:* Images of mailpieces captured during normal mail processing operations.

RECORD SOURCE CATEGORIES:
Customers and, for call center operations, commercially available sources of names, addresses, and telephone numbers.

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), logon ID, mailing address(es), 11-digit ZIP Code, or any Intelligent Mail barcode.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:
1. Records are retained for up to 30 days.
2. Records related to ePubWatch, Confirmation Services and hold mail services are retained for up to 1 year.
3. Special Services and drop ship records are retained 2 years.
4. ACH records are retained up to 2 years.
5. Mailpiece images will be retained up to 3 days.
6. Other records are retained 4 years after the relationship ends.
7. USPS and other carrier network tracking records are retained for up to 30 days for mail and up to 90 days for packages and special services.

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 266.6.

CONTESTING RECORD PROCEDURES:
See NOTIFICATIONS 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 should contain name, customer ID(s), if any, and/or logon ID.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:
None.

HISTORY:
June 05, 2017, 82 FR 25819; August 25, 2016, 81 FR 58542; January 21, 2014, 79 FR 3423; August 03, 2012, 77 FR 46528; June 27, 2012, 77 FR 38342; October 24, 2011, 76 FR 65756; April 29, 2005, 70 FR 22516.

SYSTEM NAME AND NUMBER:
USPS 820.300, Informed Delivery.

SECURITY CLASSIFICATION:
None.

SYSTEM LOCATION:
USPS Headquarters; Wilkes-Barre Solutions Center; and Eagan, MN.

SYSTEM MANAGER(S):
Vice President, Product Innovation, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260-1010, (202) 268-6078.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
39 U.S.C. 401, 403, and 404.

PURPOSE(S) OF THE SYSTEM:
1. To support the Informed Delivery notification service which provides customers with electronic notification of physical mail that is intended for delivery at the customer's address.
2. To provide daily email communication to consumers with images of the letter-size mailpieces that they can expect to be delivered to their mailbox each day.
3. To provide an enhanced customer experience and convenience for mail delivery services by linking physical mail to electronic content.
4. To obtain and maintain current and up-to-date address and other contact information to assure accurate and reliable delivery and fulfillment of postal products, services, and other material.
5. To determine the outcomes of marketing or advertising campaigns and to guide policy and business decisions through the use of analytics.
6. To identify, prevent, or mitigate the effects of fraudulent transactions.
7. To demonstrate the value of Informed Delivery in enhancing the responsiveness to physical mail and to promote use of the mail by commercial mailers and other postal customers.
8. To enhance the customer experience by improving the security of Change of Address (COA) and Hold Mail processes.
9. To protect USPS customers from becoming potential victims of mail fraud and identity theft.
10. To identify and mitigate potential fraud in the COA and Hold Mail processes.
11. To verify a customer's identity when applying for COA and Hold Mail services.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
1. Customers who are enrolled in Informed Delivery notification service.
2. Mailers that use Informed Delivery notification service to enhance the value of the physical mail sent to customers.

CATEGORIES OF RECORDS IN THE SYSTEM:
1. *Customer information:* Name; customer ID(s); mailing (physical) address(es) and corresponding 11-digit delivery point ZIP Code; phone number(s); email address(es); text message number(s) and carrier.
2. *Customer account preferences:* Individual customer preferences related to email and online communication participation level for USPS and marketing information.
3. *Customer feedback:* Information submitted by customers related to Informed Delivery notification service or any other postal product or service.
4. *Subscription information:* Date of customer sign-up for services through an opt-in process; date customer opts-out of services; nature of service provided.
5. *Data on mailpieces:* Destination address of mailpiece; Intelligent Mail barcode (IMb); 11-digit delivery point ZIP Code; and delivery status; identification number assigned to equipment

used to process mailpiece.

6. *Mail Images:* Electronic files containing images of mailpieces captured during normal mail processing operations.
7. *User Data associated with 11-digit ZIP Codes:* Information related to the user's interaction with Informed Delivery email messages, including but not limited to, email open and click-through rates, dates, times, and open rates appended to mailpiece images (user data is not associated with personally identifiable information).
8. *Data on Mailings:* Intelligent Mail barcode (IMb) and its components including the Mailer Identifier (Mailer ID or MID), Service Type Identifier (STID) and Serial Number.

RECORD SOURCE CATEGORIES:

Individual customers who request Informed Delivery notification service; *usps.com* account holders; other USPS systems and applications including those that support online change of address, mail hold services, Premium Forwarding Service, or PO Boxes Online; commercial entities, including commercial mailers or other Postal Service business partners and third-party mailing list providers.

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 and computer storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

By customer email address, 11-Digit ZIP Code and/or the Mailer ID component of the Intelligent Mail Barcode.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

1. Mailpiece images will be retained up to 7 days (mailpiece images are not associated with personally identifiable information). Records stored in the subscription database are retained until the customer cancels or opts out of the service.
2. User data is retained for 2 years, 11 months.

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

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

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. Access is controlled by logon ID and password. 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 266.6.

CONTESTING RECORD PROCEDURES:
See NOTIFICATION PROCEDURES and RECORD ACCESS PROCEDURES.

NOTIFICATION PROCEDURES:
Customers who want 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, email, and other identifying information.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:
None.

HISTORY:
August 25, 2016, 81 FR 58542.

Ruth Stevenson,
Attorney, Federal Compliance.
[FR Doc. 2018-27965 Filed: 12/26/2018 8:45 am; Publication Date: 12/27/2018]