



December 12, 2013

Mr. Rich Jones
MuckRock News
DEPT MR 5970
PO Box 55819
Boston, MA 02205-5819

RE: FOIA Case No. 2013-FPRO-819

Dear Mr. Jones:

This is in further reference to your Freedom of Information Act (FOIA) request dated June 10, 2013, in which you seek access to Postal Service records. Specifically, you request any and all documents detailing Mail Isolation Control and Tracking (MICT) procedures.

We note that you have requested a fee waiver due to the public interest. You state in your letter that the documents will be made available to the general public free of charge as part of the public information service at MuckRock.com, processed by a representative of the news media/press and is made in the process of news gathering and not for commercial usage.

With respect to your fee waiver request, although you submitted your request through MuckRock.com, a website which serves as a request proxy, you have not demonstrated how you are actively gathering news for an entity that disseminates news to the public. Should you choose to modify your FOIA request, your fee waiver request must describe all of the following: how the information will be used; to whom it will be provided, including the public; how the public is to benefit from the disclosure; any personal or commercial benefit that the requester expects from disclosure; and your identity, qualifications, and expertise in the subject area.

Absent the required information to consider a fee waiver request, we will consider that you are within the category of "other requesters" as defined by Postal Service FOIA fee regulations. This category applies to requesters who are not commercial use requesters, educational or scientific requesters, or news media requesters. Requests in the "other" category are entitled to two free hours of search time and 100 pages of free duplication. Fees totaling less than \$10 are waived. Requesters are notified in advance of all costs expected to exceed \$25.00 if they have not indicated their willingness to accept costs that may be incurred in processing their request.

The Freedom of Information Act (FOIA), 5 USC §552, is a records and document statute. Identification of the record(s) desired is the responsibility of the requester. The FOIA (5 U.S.C. 552(a)(3)(A)) requires the requester to reasonably describe the records being sought. A description is considered reasonable if it permits an agency employee who is familiar with the subject area to locate the requested records with a "reasonable" amount of effort. It is the requester's responsibility to frame requests with sufficient particularity to ensure that searches are not unreasonably burdensome, and to enable the searching agency to determine precisely what records are being requested.

In your records request, you request relevant contracts, purchase orders and locations of physical hardware regarding MICT procedures. As explained below, MICT is a set of safety procedures that utilizes existing automated mail processing equipment. Accordingly, the Postal Service does not have any records concerning this portion of your request.

Regarding your request for any and all emails, memos, PowerPoint Presentations and requests for system access by the FBI or any other federal agency" detailing MICT, we have determined that responsive records would be maintained by the following Headquarters departments: Operations, Engineering, Postal Inspection Service, General Counsel, Government Relations, Privacy Office and Supply Management. Please be advised that, while we wish to fully cooperate in processing your request, your letter does not provide sufficient detail to allow for the ready identification and retrieval of the desired documents. We note that you did not limit your search to a particular office or department, report or document type or to a particular timeframe.

Accordingly, we will need more definitive information concerning the records you seek. Such a description will ensure responsible use of postal resources to satisfy your right to access. If you can provide additional information to identify the specific documents you seek, you may resubmit your request to this office.

Consequently, given that your request cannot be processed as formulated, we plan to take no further action unless we hear back from you within 30 days from the date of this letter. Should you have questions or need assistance in reformulating your request, please contact me at (314) 345-5846.

In an effort to help you potentially clarify the documents you may be specifically interested in reviewing, we offer the following information:

After some confusing reports appeared in the media, the Postal Service received a series of similar FOIA requests that seek information regarding what are actually three distinct USPS processes and or programs.

Some of those requests address what are generally referred to as "mail covers." The mail cover program is a long established law enforcement tool that is administered by the Postal Inspection Service and governed by regulations published in the Code of Federal Regulations.

A separate process that was discussed in the media was "mail imaging." "Mail imaging" performed by USPS automation equipment is an operational tool that was developed in the 1990's specifically to enable the automated sortation of mail and thereby maximize efficiency and potential cost savings. The vast majority of digital images created by USPS automation equipment simply serve a processing function and they are maintained for less than three minutes. However, some of those mail images can be retained for longer periods of time based on specific requests made to meet a variety of USPS operational needs, which are described in the below narrative and referenced or attached USPS regulations. Otherwise, the Postal Service does not routinely compile those digital images of mail and it does not store them in a central database.

Finally, some media reports and subsequent FOIA requests appear to confuse routine "mail imaging" done by Postal Service mail processing automation equipment with MICT procedures. MICT is a set of safety procedures that were developed in response to the anthrax attacks that occurred in October of 2001 and the subsequent deployment of Biohazard Detection System technology to detect anthrax in the mail. The objective of MICT and mail tracking that occurs in the event of other serious suspicious mail incidents is to ensure a coordinated response to potentially hazardous mail in order to protect employees and the public.

MAIL COVERS:

The mail cover program is described in great detail in the Code of Federal Regulations (CFR). A mail cover is a process undertaken specifically for law enforcement purposes that involves the recording of mail matter. In 39 CFR § 233.3 a "mail cover" is defined as "the process by which a nonconsensual record is made of any data appearing on the outside cover of any sealed or unsealed class of mail matter, or by which a record is made of the contents of any unsealed class

of mail matter as allowed by law.” Postal regulations relating to mail covers can be traced back to the 1890s. Initially, the technique was intended as a law enforcement tool to locate fugitives. The regulations were first published in the Code of Federal Regulations in 1975 in order “to make these regulations more accessible to the public, and to discourage confusion concerning the nature and uses of this important law enforcement tool.” The regulations note that the USPS “maintains rigid control and supervision with respect to the use of mail covers as an investigative technique for law enforcement or the protection of national security.” 39 CFR § 233.3(a).

The Chief Postal Inspector is the “principal officer” of the Postal Service in the administration of all matters governing mail covers. 39 CFR § 233.3(d). Pursuant to the regulations codified at 39 CFR § 233.3 (e)(1) and (2), mail covers may be ordered under the following circumstances:

1. When a written request is received from a postal inspector that states reason to believe a mail cover will produce evidence relating to the violation of a postal statute.
2. When a written request is received from any law enforcement agency in which the requesting authority specifies the reasonable grounds to demonstrate the mail cover is necessary to:
 - To protect national security
 - To locate a fugitive
 - To obtain evidence of the commission or attempted commission of a crime
 - To assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law.

The courts have upheld the use of the mail cover program, finding in part that mail covers do not violate privacy rights because there is no expectation of privacy for the information on the outside of a piece of mail.

OPERATIONAL MAIL IMAGING

In the early 1990's, the Postal Service began using “mail imaging” and developing optical character reader technology to maximize efficient processing and delivery of the mail. Mail imaging technology enabled the Postal Service to apply barcodes on mail pieces that allow automated sortation by machines that can read those barcodes. As automated mail machinery replaced manual handling and sortation by employees it significantly reduced costs and improved delivery service times.

As part of USPS automation technology, individual mail processing machines create images that are generally maintained for a matter of minutes while they are utilized for mail sortation. Under some limited circumstances, certain digital images that meet requested specifications can be gathered and retained for periods of time up to 120 days to be used for a variety of operational, revenue protection, law enforcement and other authorized purposes. Postal regulations set forth in the USPS Administrative Support Manual (ASM), Subpart 274.5 (see the copy attached) address and limit the use of these images. Contrary to some media reports, the Postal Service does not have a central database of mail piece images, nor does the Postal Service use mail piece images to monitor the mailing habits of any individual or group.

MAIL ISOLATION, CONTROL AND TRACKING (“MICT”)

MICT describes a set of safety procedures developed by the Postal Service in response to the anthrax mailings that occurred in October 2001. The objective of MICT is to ensure a complete and coordinated response to a Biohazard Detection System (BDS) alert through the isolation and control of potentially contaminated mail in an alerting plant, or through recall of Postal transportation vehicles to that plant, and subsequent tracking to identify the suspect piece(s) and

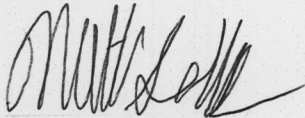
determine the path taken in the Postal system. Mail tracking also occurs in the event of some other serious suspicious mail incidents where a risk assessment concludes that there may be employee and public health concerns. Under such circumstances, all possible steps are taken to protect the safety and security of employees and the public. Tracking procedures use all existing operational data and available technology to trace the path of the suspicious mail piece so that the facilities, vehicles and processing machines that came in contact with a suspected mail piece can be identified and appropriate safety measures can then be taken with regard to each of them.

Generally, these tasks are accomplished by using the serialization barcode information that is placed on a letter by a mail processing machine in order to determine the other machines that were used in its processing. The mail images obtained for mail processing purposes, if available, can also be utilized as a part of the tracking process to learn more information about the suspicious mail piece (such as the return address), and to determine whether any other, similar suspicious mail pieces were processed through the system during the relevant period. Some newer processing equipment has the capability to archive images within its memory for a short period of time. Availability of mail processing related images depends upon the amount of time that has transpired between the time the mail was processed and the time an investigation occurs. By way of example, this technology helped Postal Inspectors locate additional suspicious mail pieces associated with a letter believed to contain ricin that went through the Postal processing system earlier this year. Information obtained in the process, such as a return address, can also have law enforcement applications under these circumstances.

The Postal Service only implements MICT procedures once a potentially hazardous mail piece is identified and brought to the attention of Postal Inspectors, either as the result of a BDS alert, or through notification by external law enforcement entities. Once MICT procedures are implemented, Postal regulations set forth in ASM Subpart 274.5k limit the use of mail images for this purpose. The Postal Service carries out MICT procedures on a local basis as the need arises and it does not have a central database of the related mail images or information.

If you consider my response to be a denial of your request, you may administratively appeal by writing to the General Counsel, U.S. Postal Service, 475 L'Enfant Plaza SW, Washington DC 20260, within 30 days of the date of this letter. The letter of appeal should include a statement about the action or failure to act being appealed, the reasons why it is believed to be erroneous, and the relief sought, along with copies of your original request, this letter, and any other related correspondence.

Sincerely,



Nathan T Solomon
Postal Attorney
USPS Law Department
1720 Market Street, Room 2400
St. Louis, MO 63155-9948
Phone: (314)345-5846
Fax: (314)345-5893

reward under this section for information obtained while so employed. The Chief Inspector may establish such procedures and forms as may be desirable to give effect to this section including procedures to protect the identity of persons claiming rewards under this section.

[36 FR 4673, Mar. 12, 1971, as amended at 42 FR 43836, Aug. 31, 1977. Redesignated at 46 FR 34330, July 1, 1981, and amended at 47 FR 26832, June 22, 1982; 47 FR 46498, Oct. 19, 1982; 49 FR 15191, Apr. 18, 1984; 54 FR 37795, Sept. 13, 1989; 55 FR 32251, Aug. 8, 1990; 59 FR 5326, Feb. 4, 1994; 60 FR 54305, Oct. 23, 1995; 63 FR 52160, Sept. 30, 1998; 69 FR 16166, Mar. 29, 2004]

§ 233.3 Mail covers.

(a) *Policy.* The U.S. Postal Service maintains rigid control and supervision with respect to the use of mail covers as an investigative technique for law enforcement or the protection of national security.

(b) *Scope.* These regulations constitute the sole authority and procedure for initiating a mail cover, and for processing, using and disclosing information obtained from mail covers.

(c) *Definitions.* For purpose of these regulations, the following terms are hereby defined.

(1) *Mail cover* is the process by which a nonconsensual record is made of any data appearing on the outside cover of any sealed or unsealed class of mail matter, or by which a record is made of the contents of any unsealed class of mail matter as allowed by law, to obtain information in order to:

- (i) Protect national security,
- (ii) Locate a fugitive,
- (iii) Obtain evidence of commission or attempted commission of a crime,
- (iv) Obtain evidence of a violation or attempted violation of a postal statute, or
- (v) Assist in the identification of property, proceeds or assets forfeitable under law.

(2) For the purposes of § 233.3 *record* is a transcription, photograph, photocopy or any other facsimile of the image of the outside cover, envelope, wrapper, or contents of any class of mail.

(3) *Sealed mail* is mail which under postal laws and regulations is included within a class of mail maintained by the Postal Service for the transmission of letters sealed against inspection.

Sealed mail includes: First-Class Mail; Priority Mail; Express Mail; Express Mail International; Global Express Guaranteed items containing only documents; Priority Mail International flat-rate envelopes and small flat-rate boxes; International Priority Airmail, except M-bags; International Surface Air Lift, except M-bags; First-Class Mail International; Global Bulk Economy, except M-bags; certain Global Direct mail as specified by customer contract; and International Transit Mail.

(4) *Unsealed mail* is mail which under postal laws or regulations is not included within a class of mail maintained by the Postal Service for the transmission of letters sealed against inspection. Unsealed mail includes: Periodicals; Standard Mail; Package Services; incidental First-Class Mail attachments and enclosures; Global Express Guaranteed items containing non-documents; Priority Mail International, except flat-rate envelopes and small flat-rate boxes; International Direct Sacks—M-bags; certain Global Direct mail as specified by customer contract; and all items sent via “Free Matter for the Blind or Handicapped” under 39 U.S.C. 3403-06 and International Mail Manual 270.

(5) *Fugitive* is any person who has fled from the United States or any State, the District of Columbia, territory or possession of the United States, to avoid prosecution for a crime, to avoid punishment for a crime, or to avoid giving testimony in a criminal proceeding.

(6) *Crime*, for the purposes of this section, is any commission of an act or the attempted commission of an act that is punishable by law by imprisonment for a term exceeding one year.

(7) *Postal statute* refers to a statute describing criminal activity, regardless of the term of imprisonment, for which the Postal Service has investigative authority, or which is directed against the Postal Service, its operations, programs, or revenues.

(8) *Law enforcement agency* is any authority of the Federal Government or any authority of a State or local government, one of whose functions is to:

- (i) Investigate the commission or attempted commission of acts constituting a crime, or

United States Postal Service

(ii) Protect the national security.

(9) *Protection of the national security* means to protect the United States from any of the following actual or potential threats to its security by a foreign power or its agents:

(i) An attack or other grave, hostile act;

(ii) Sabotage, or international terrorism; or

(iii) Clandestine intelligence activities, including commercial espionage.

(10) *Emergency situation* refers to circumstances which require the immediate release of information to prevent the loss of evidence or in which there is a potential for immediate physical harm to persons or property.

(d) *Authorizations—Chief Postal Inspector.* (1) The Chief Postal Inspector is the principal officer of the Postal Service in the administration of all matters governing mail covers. The Chief Postal Inspector may delegate any or all authority in this regard to not more than two designees at Inspection Service Headquarters.

(2) Except for national security mail covers, the Chief Postal Inspector may also delegate any or all authority to the Manager, Inspection Service Operations Support Group, and, for emergency situations, to Inspectors in Charge. The Manager, Inspection Service Operations Support Group, may delegate this authority to no more than two designees at each Operations Support Group.

(3) All such delegations of authority shall be issued through official, written directives. Except for delegations at Inspection Service Headquarters, such delegations shall only apply to the geographic areas served by the Manager, Inspection Service Operation Support Group, or designee.

(e) The Chief Postal Inspector, or his designee, may order mail covers under the following circumstances:

(1) When a written request is received from a postal inspector that states reason to believe a mail cover will produce evidence relating to the violation of a postal statute.

(2) When a written request is received from any law enforcement agency in which the requesting authority specifies the reasonable grounds to demonstrate the mail cover is necessary to:

(i) Protect the national security,

(ii) Locate a fugitive,

(iii) Obtain information regarding the commission or attempted commission of a crime, or

(iv) Assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law.

(3) When time is of the essence, the Chief Postal Inspector, or designee, may act upon an oral request to be confirmed by the requesting authority in writing within three calendar days. Information may be released by the Chief Postal Inspector or designee, prior to receipt of the written request, only when the releasing official is satisfied that an emergency situation exists.

(f)(1) *Exceptions.* A postal inspector, or a postal employee acting at the direction of a postal inspector, may record the information appearing on the envelope or outer wrapping, of mail without obtaining a mail cover order, only under the circumstances in paragraph (f)(2) of this section.

(2) The mail must be:

(i) Undelivered mail found abandoned or in the possession of a person reasonably believed to have stolen or embezzled such mail,

(ii) Damaged or rifled, undelivered mail, or

(iii) An immediate threat to persons or property.

(g) *Limitations.* (1) No person in the Postal Service except those employed for that purpose in dead-mail offices, may open, or inspect the contents of, or permit the opening or inspection of sealed mail without a federal search warrant, even though it may contain criminal or otherwise nonmailable matter, or furnish evidence of the commission of a crime, or the violation of a postal statute.

(2) No employee of the Postal Service shall open or inspect the contents of any unsealed mail, except for the purpose of determining:

(i) Payment of proper postage, or

(ii) Mailability.

(3) No mail cover shall include matter mailed between the mail cover subject and the subject's known attorney.

(4) No officer or employee of the Postal Service other than the Chief Postal Inspector, Manager, Inspection

Service Operations Support Group, and their designees, are authorized to order mail covers. Under no circumstances may a postmaster or postal employee furnish information as defined in § 233.3(c)(1) to any person, except as authorized by a mail cover order issued by the Chief Postal Inspector or designee, or as directed by a postal inspector under the circumstances described in § 233.3(f).

(5) Except for mail covers ordered upon fugitives or subjects engaged, or suspected to be engaged, in any activity against the national security, no mail cover order shall remain in effect for more than 30 days, unless adequate justification is provided by the requesting authority. At the expiration of the mail cover order period, or prior thereto, the requesting authority may be granted additional 30-day periods under the same conditions and procedures applicable to the original request. The requesting authority must provide a statement of the investigative benefit of the mail cover and anticipated benefits to be derived from its extension.

(6) No mail cover shall remain in force longer than 120 continuous days unless personally approved for further extension by the Chief Postal Inspector or designees at National Headquarters.

(7) Except for fugitive cases, no mail cover shall remain in force when an information has been filed or the subject has been indicted for the matter for which the mail cover is requested. If the subject is under investigation for further criminal violations, or a mail cover is required to assist in the identification of property, proceeds or assets forfeitable because of a violation of criminal law, a new mail cover order must be requested consistent with these regulations.

(8) Any national security mail cover request must be approved personally by the head of the law enforcement agency requesting the cover or one designee at the agency's headquarters level. The head of the agency shall notify the Chief Postal Inspector in writing of such designation.

(h) *Records.* (1) All requests for mail covers, with records of action ordered thereon, and all reports issued pursuant thereto, shall be deemed within the custody of the Chief Postal Inspector.

However, the physical storage of this data shall be at the discretion of the Chief Postal Inspector.

(2) If the Chief Postal Inspector, or his designee, determines a mail cover was improperly ordered, all data acquired while the cover was in force shall be destroyed, and the requesting authority notified of the discontinuance of the mail cover and the reasons therefor.

(3) Any data concerning mail covers shall be made available to any mail cover subject in any legal proceeding through appropriate discovery procedures.

(4) The retention period for files and records pertaining to mail covers shall be 8 years.

(i) *Reporting to requesting authority.* Once a mail cover has been duly ordered, authorization may be delegated to any employee in the Postal Inspection Service to transmit mail cover reports directly to the requesting authority.

(j) *Review.* (1) The Chief Postal Inspector, or his designee at Inspection Service Headquarters shall periodically review mail cover orders issued by the Manager, Inspection Service Operations Support Group or their designees to ensure compliance with these regulations and procedures.

(2) The Chief Postal Inspector shall select and appoint a designee to conduct a periodic review of national security mail cover orders.

(3) The Chief Postal Inspector's determination in all matters concerning mail covers shall be final and conclusive and not subject to further administrative review.

(k) *Military postal system.* Section 233.3 does not apply to the military postal system overseas or to persons performing military postal duties overseas. Information about regulations prescribed by the Department of Defense for the military postal system overseas may be obtained from the Department of Defense.

[58 FR 36599, July 8, 1993, as amended at 61 FR 42557, Aug. 16, 1996; 74 FR 18297, Apr. 22, 2009]

§ 233.4 Withdrawal of mail privileges.

(a) *False representation and lottery orders*—(1) *Issuance.* Pursuant to 39 U.S.C.

3005, the Judicial Officer of the Postal Service, acting upon a satisfactory evidentiary basis, may issue a mail-stop order against anyone seeking mailed remittance of money or property by means of a false-representation or lottery scheme. Such orders provide for return of mail and refund of postal money orders to remitters.

(2) *Enforcement.* Notice of these orders, including any necessary instructions on enforcement responsibilities and procedures, is published in the Postal Bulletin. Generally, an order against a domestic enterprise is enforced only by the post office designated in the order. All personnel processing mail for dispatch abroad assist in enforcing orders against foreign enterprises by forwarding mail addressed to such enterprises to designated post offices.

(b) *Fictitious name or address and not residents of the place of address orders—*

(1) *Issuance.* Pursuant to 39 U.S.C. 3003, 3004, when there is satisfactory evidence that mail is addressed to a fictitious name, title, or address used for any unlawful business, and no one has established a right to have the mail delivered to him, or that mail is addressed to places not the residence or regular business address of the person for whom they are intended to enable the person to escape identification, the Judicial Officer may, pursuant to Part 964, order that the mail be returned to the sender.

(2) *Notice.* (i) The Chief Postal Inspector or his delegate must give notice to the addressee of mail withheld from delivery pursuant to 39 U.S.C. 3003, 3004 that such action has been taken and advise him that he may:

(A) Obtain such mail upon presenting proof of his identity and right to receive such mail, or

(B) Petition the Judicial Officer for the return of such mail. (ii) The notice must be in writing and served by personal service upon the addressee or by Certified Mail (Return Receipt Requested) and by First Class Mail.

(3) *Enforcement.* Notice of any order issued pursuant to 39 U.S.C. 3003, 3004, and any necessary implementing in-

structions, are published in the Postal Bulletin.

[45 FR 1613, Jan. 8, 1980. Redesignated at 46 FR 34330, July 1, 1981, and amended at 53 FR 1780, Jan. 22, 1988]

§ 233.5 Requesting financial records from a financial institution.

(a) *Definitions.* The terms used in this section have the same meaning as similar terms used in the Right to Financial Privacy Act of 1978, Title XI of Pub. L. 95-630. *Act* means the *Right to Financial Privacy Act of 1978*.

(b) *Purpose.* The purpose of these regulations is: (1) To authorize the Inspection Service Department of the U.S. Postal Service to request financial records from a financial institution pursuant to the formal written request procedure authorized by section 1108 of the Act and (2) to set forth the conditions under which such request may be made.

(c) *Authorization.* The Inspection Service Department is authorized to request financial records of any customer from a financial institution pursuant to a formal written request under the Act only if:

(1) No administrative summons or subpoena authority reasonably appears to be available to the Inspection Service Department to obtain financial records for the purpose for which the records are sought;

(2) There is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry and will further that inquiry;

(3) The request is issued by a supervisory official of a rank designated by the Chief Postal Inspector. Officials so designated shall not delegate this authority to others;

(4) The request adheres to the requirements set forth in paragraph (d) of this section; and

(5) The notice requirements set forth in section 1108(4) of the Act, or the requirements pertaining to the delay of notice in section 1109 of the Act, are satisfied, except in situations (*e.g.*, section 1113(g)) where no notice is required.

(d) *Written request.* (1) The formal request must be in the form of a letter or memorandum to an appropriate official

- e. After screening conducted under this subsection, mail that is reasonably suspected of posing an immediate and substantial danger to life or limb, or an immediate and substantial danger to property, may be treated by postal employees as provided in 274.42.
- f. After screening, mail sealed against inspection that presents doubts about whether its contents are hazardous, that cannot be resolved without opening, must be reported to the Postal Inspection Service. Such mail must be disposed of under instructions promptly furnished by the Postal Inspection Service.

274.42 **Threatening Pieces of Mail**

Mail, sealed or unsealed, reasonably suspected of posing an immediate danger to life or limb or an immediate and substantial danger to property may, without a search warrant, be detained, opened, removed from postal custody, and processed or treated, but only to the extent necessary to determine and eliminate the danger and only if a complete written and sworn statement of the detention, opening, removal, or treatment, and the circumstances that prompted it, signed by the person purporting to act under this subsection, is promptly forwarded to the chief postal inspector.

274.43 **Reports**

Any person purporting to act under this subsection who does not report his or her action to the chief postal inspector under the requirements of this subsection, or whose action is determined after investigation not to have been authorized, is subject to disciplinary action or criminal prosecution, or both.

274.5 **Disclosure of Information Collected From Mail Sent or Received by Customers**

As a general rule, Postal Service employees may not disclose information or data from the exterior of a piece of mail, disclose information about the contents of a piece of mail, or disclose other information about a piece of mail, within or outside the Postal Service. Only under the following conditions may an employee disclose information while performing official duties:

- a. To the Postal Inspection Service or Office of the Inspector General (OIG) for its official use, when there is a reasonable basis to suspect that the information is evidence of the commission of a crime.
- b. In accordance with 213, Mail Covers.
- c. As mandated by a search warrant and in accordance with 274.6, Execution of Search Warrants.
- d. As mandated by a federal court order.
- e. To fulfill the request of the sender, addressee, or an authorized agent of the sender or addressee.
- f. For the following Postal Service operations, employees may make, record, or disclose an image of a mailpiece. Any image created for Postal Service operations must be destroyed once the information is no longer necessary for that operational purpose:
 - (1) To resolve or record a service complaint when the complaining customer presents the mail piece or image as evidence.

- j. To law enforcement personnel charged with investigating and enforcing compliance with U.S. export or assets controls, with respect to mailpieces identified as potentially violating U.S. export control or assets control laws.
- k. The Postal Service may record mail images to ensure the health or safety of Postal Service employees or the public. However, the Postal Service may only keep the images for 60 days or less, unless the Chief Postal Inspector extends the time. Such information may not be used for criminal investigative purposes without following the policy and procedures in part 213 regarding mail covers.
- l. The Postal Service or authorized third party may open, read, and respond to mail, or contact the sender, regarding correspondence that is addressed to "Santa Claus," "the North Pole," or similar seasonal characters or destinations and which would otherwise be undeliverable as addressed.
- m. If otherwise permitted by law.

274.51 **Disclosure of Information from Contents of Sealed Mail**

Information obtained by opening sealed mail in a mail recovery center may only be used to find and identify an address to which the Postal Service can deliver the mail, except:

- a. As mandated by a search warrant and in accordance with 274.6, Execution of Search Warrants.
- b. As mandated by a federal court order.
- c. To fulfill the request of the sender, addressee, or an authorized agent of the sender or addressee.

274.6 **Execution of Search Warrants**

274.61 **Warrant Issued by Federal Court or Served by Federal Officer**

- a. A search warrant duly issued under Rule 41 of the Federal Rules of Criminal Procedure must be executed as provided in 274.62. Usually, a warrant issued by a federal court or served by a federal officer is issued under Rule 41, and is duly issued if signed and dated within the past 10 days.
- b. No employee may permit the execution of a search warrant issued by a state court and served by a state officer. If in doubt, an employee should temporarily detain the mail in question and promptly call a postal inspector for guidance.

274.62 **Search Warrant Execution Procedures**

Procedures for executing a search warrant follow:

- a. A postal inspector may execute a search warrant.
- b. An OIG special agent may execute a search warrant.
- c. A person other than a postal inspector or OIG special agent executing a search warrant must be accompanied by a postal employee authorized by the head of the postal installation at which the warrant is to be executed.