Before The

POSTAL RATE COMMISSION

WASHINGTON, D.C. 20268-0001

Complaint on Electronic Postmark® Docket No. C2004-2

SURREBUTTAL TESTIMONY OF RICK BORGERS ON BEHALF OF DIGISTAMP, INC.

(September 14, 2006)

Table of Contents

The* USPS EPM® *is a document delivery service.

During oral cross-examination, Mr. Foti gave confused, confusing, and contradictory testimony on the question of whether the USPS is part of, incidental, or ancillary to, document delivery.

> Page 183 [1]
>
> Q. MR BORGERS Okay. The document, the Microsoft Word document, was on my computer. I used USPS EPM software. Was that document transferred to the Data Center at the U.S. Postal Service whereby it was attached to this email and then forwarded on my behalf to Chris Casady?
> A. MR FOTI Could you repeat the question?
> Q We started this demonstration with a Microsoft Word document. I used EPM software to designate who I wanted that document to be delivered to. Is it correct in fact that that Microsoft Word document was transferred from my computer to the U.S. Postal Service Data Center at which point it was attached to an email from the U.S. Postal Service and sent to chriscasady@digistamp.com?
> A That document is never received by the USPS server.

In fact, Mr. Foti's statement is simply false, and later he corrects this mistake:

> Page 227
>
> Q. MR BORGERS Please, Mr. Foti, given the research you were able to over the break is it true that the document that was used in my demo, did it travel from the sender's computer directly to the receiver's computer or did it in fact go to U.S. Postal Service's Data Center prior to being sent to the recipient?
> A. MR FOTI It's my understanding that the encrypted documents may go through a postal data center, but not through the EPM service.
> Q So let me see if I understand. So the Microsoft Word document traveled from the sender's computer to a computer owned and operated by the Postal Service and then was forwarded to the designated recipient?
> A The encrypted document went through the USPS Postal Data Center.
> Q From there it went to the recipient?
> A I believe so. Yes

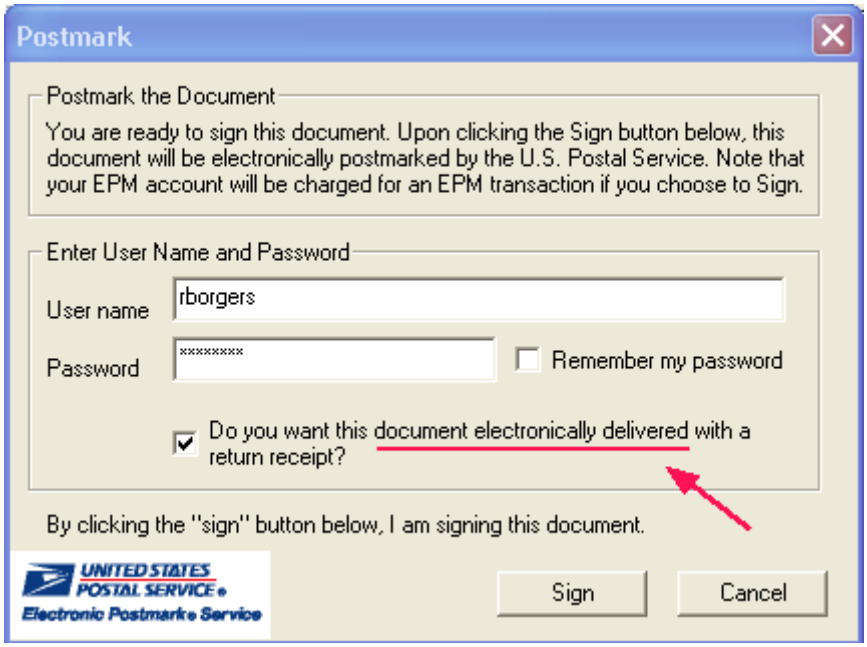
Yet later, Mr. Foti seems to reverse himself yet again:

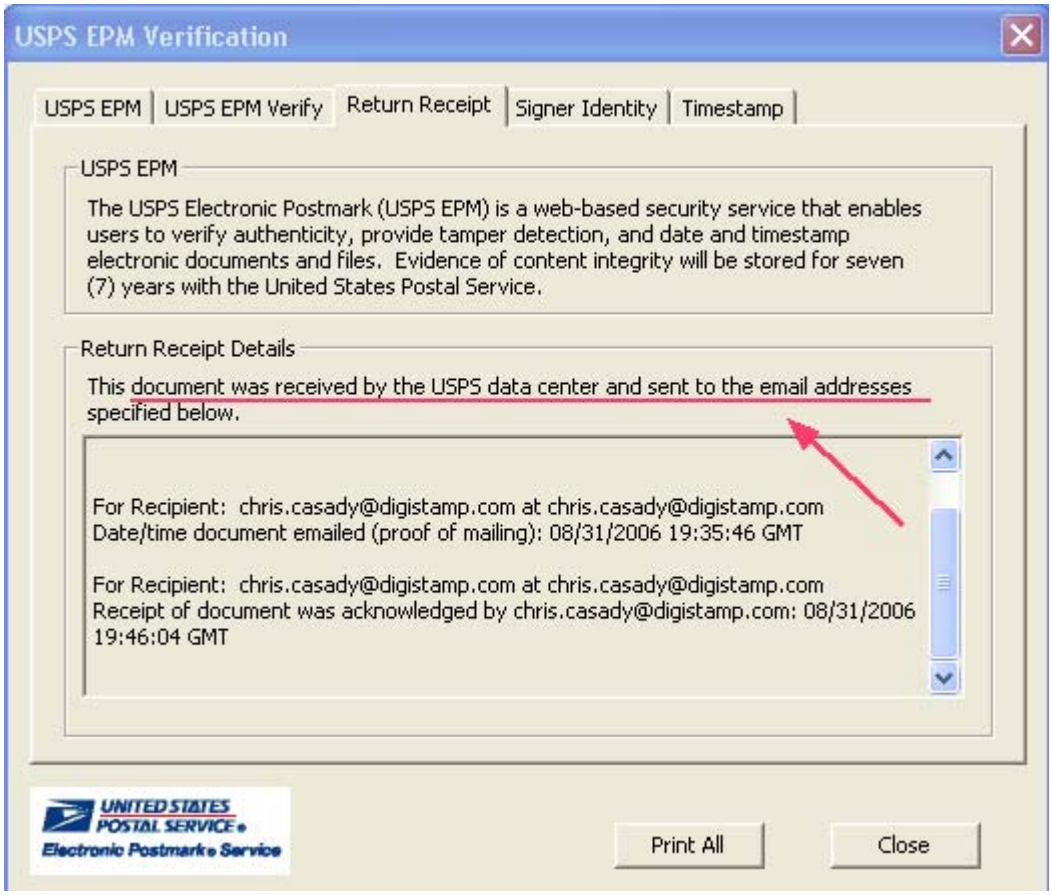
> Page 271

[1] Volume 1 - Official Transcript of the Hearing Held on August 15, 2006

Q. MR BORGERS Very good. This is much like a piece of mail that I put my return address on and it gets to the recipient, the addressee. Yes, you can see who addressed the envelope, but in fact the Postal Service delivered the Microsoft Word document. Is that not true?
A. MR FOTI The Postal Service authenticated the document. It was provided through another service provider.
Q Okay. The document is an attachment on an email that came from a computer at the U.S. Postal Service Data Center. Effectively did not you, the Postal Service, deliver this Microsoft Word document as an attachment on an email from the Postal Service?
A We did not deliver any document.
Q The document came from a computer at the Postal Service. That was the step before it got here.
A It traveled to some sort of transport. We do not deliver the document.
MR. BORGERS: I don't know how to make that any clearer, so I will stop at that point.

Mr. Foti's confusion is very odd, since the answer to the question is an integral part of ordinary use of the EPM. When a customer uses the "USPS EPM free software" to send an EPMed document, these two screens (messages) are part of the process:





It is simply true that for the everyday use of a USPS EPM by any ordinary customer, the customer's document is sent to the Postal Service. The Postal Service then creates an email, attaches the document and delivers the document to the address specified by the sender.

It is simply false to say, as the USPS has said, that the electronic postmark service is not a postal service because it does not deliver anything between senders and recipients.[2]

It is simply false to say, as the USPS has said, that that electronic postmark service neither requires nor accomplishes the transmission of content. *Id.* at 14.

Thus, there can be no merit to Postal Service argument that, since nothing moves between the sender and recipient, "it is impossible to construe any 'carriage of mail' that is the sine qua non of a postal service." *Id.* 14-15.

[2] Motion of the United States Postal Service to Dismiss at 12-13

In passing we should note that Mr. Foti argued that the free software of which the two screens cited above are part "is just a plug-in and not the EPM" and argued "less that 1 percent of the customers use this plug-in."

But that is completely beside the point. The truth only has to be told once, by or to one person, to be known. In fact, the messages to the consumer included in this plug-in reveal clearly exactly what happens with an EPM.

For clarity, it is also good to note that the plug-in that Mr. Foti refers to is sold to the consumer as *USPS EPM® Extension for Microsoft® Office.* This name is clearly stated on the USPS web site and has been marketed as such for several years.

Even if programmers were to rewrite the plug-in to hide these facts, as Mr. Foti may wish had already been done, they are facts. That the Microsoft plug-in reveals clearly facts about how the EPM works suggests that Mr. Foti's testimony before the Commission is tailored to make a point to the Commission -- not to state the plain facts that the programmers who wrote the plug-in, the USPS data center operators, and the customers who use it, know quite well.

The citing of HIPAA[3] rules is a red herring unrelated to any issue before the Commission.

In both written and oral testimony, Mr. Foti has cited HIPAA rules to contend that a fax is not an electronic communication—and therefore, since the overwhelming majority of EPMs are purchased by a single customer who uses them to authenticate fax orders for medical equipment, the EPM is not part of a process of communication. I believe this properly summarizes Mr. Foti's testimony on this subject:

Page 205 [4]

[3] HIPAA stands for the "Health Insurance Portability and Accountability Act of 1996," Public Law 104-191. The Department of Health and Human Services is required (under the HIPAA statutes) to establish national standards for security and privacy. Mr. Foti in his oral testimony quoted § 160.103 *Definitions* of the February 20, 2003 Rules and Regulations stored here: http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf see page 42 / 8374

Q Okay. Very good. I need to restate a question. The doctor's orders that are sent to this medical device provider, they're sent to them via fax. Is this an example of an electronic communication?
A Again, you've asked me that, and I told you I could dispute that. I think I have.
Q I didn't ask whether you could dispute it. I asked you in the specific example of this situation where doctor's orders are faxed to this medical supplier is this an example of an electronic communication?
A Based on HIPAA rules, I'm going to say no.

Page 213 – 214

Q We have established, I do believe, and correct me if I'm wrong. Is it true that we have established that this customer has a system that receives faxes that are electronic communication?
A Again, I could dispute whether or not faxes are electronic communication.
Q But for this customer --
A And I think I did for this customer also.

I regret that I did not realize, prior to examining Mr. Foti, that this line of reasoning is specious.

The HIPAA rules are designed to distinguish **which media are electronic and which are not**—that is, which forms of communication fall under a certain set of federal rules governing security of information; so the question of whether fax orders are, or are not, ***electronic***, is the HIPAA issue.

But that is not the issue before the Commission. The issue before the Commission is whether the EPM is integral, incidental, or ancillary to ***communication***.

The HIPAA rules simply do not address whether a fax is an act of communication. They are, therefore, beside the point.

Mr. Foti's argument is that, since HIPAA (according to his interpretation) does not see a fax as an electronic communication, it is not a communication. But that

[4] Volume 1 - Official Transcript of the Hearing Held on August 15, 2006

conclusion is not even at issue in the HIPAA regulations, and they have nothing to say to support that conclusion.

Mr. Foti's argument is formally identical to the following:

> A crow is not a greenish-blue bird; therefore, a crow is not a bird.

We need not argue over how to interpret the HIPAA rules, or how they apply to the current case. Mr. Foti's argument simply is absurd, and I apologize to the Commission for having allowed myself to be misled, and for having wasted the Commission's time with unproductive cross-examination on this issue.

No one in his or her right mind can honestly deny that a fax is an act of communication[5].

No one who examines the USPS fax-authentication product can deny that it is integrated into the fax process.

Therefore, no one can reasonably deny that the USPS EPM, as used by its largest customer, is integrated into, and therefore certainly part of, an act of communication.

It follows that the USPS EPM as used by its largest customer is a postal service as defined by the Commission.

[5] Though HIPAA is irrelevant to the case before the Commission, I would note that everyone knows that a fax is, in fact, an electronic communication. See Appendix A for quotes from:

- United States Postal Service
- US Postal Service Inspectors
- United States Attorneys' Manual
- 18 U.S.C. § 2510(12)
- 18 U.S.C. § 1341 and § 1343
- U. S. Food and Drug Administration
- American Bar Association
- Authentidate, USPS EPM contractor

The USPS obfuscates the nature of* USPS EPM® *by reference to one customer.

The USPS would like the Commission to believe that the principal market for EPMs is fax-related security. However, this is highly misleading, an artifact of the USPS having one large customer that uses the EPM in this way.

Consider a direct analogy: A company distributes bottles of water for water coolers. It has never managed to generate many big clients, instead selling a couple of bottles a month to lots of little businesses and some upscale homes. But a new hospital is built next door to the company warehouse, and the company bids to supply bottled water to the hospital. The company wins the contract! Suddenly, eighty-five percent of its business is with the hospital. The owner starts telling people, "I don't sell water--I'm in the medical supply business."

But the water salesman sells water, and the EPM is an electronic postmark, even when one large customer signs on for a specific use.

The USPS would like the Commission to believe that the use of the EPM to guarantee the accurate transmission, recording, and processing of medical-related communications via fax-to-computer processes is a “business process,” not a process of transmitting data from one party to another.

This is misleading. While it is true that the recipient’s computer requests and attaches the EPM to the received electronic file (and we should note that it is impossible to attach an EPM to something that is *not* an electronic file, located on a computer), the communication between sender and recipient cannot be completed without the EPM being attached. That is why the EPM is useful as a security measure. If the recipient could access the information in the file without the EPM’s being attached, the file simply would not be secure, and the EPM would serve no purpose in the transfer of information from sender to recipient.

This cannot be emphasized too highly: communication is a flow of information from one party to another. The physical location—like the physical materials or physical configuration—of appliances used to accomplish that flow of information is logically irrelevant to the flow of information itself. Computer scientists use the image of a “flow of information,” and the location of a process within the “stream” in order to make the point that physical embodiment is irrelevant.

Only when information has been ***sent and received in an accessible form*** has communication happened. And the fax customer simply, unequivocally ***cannot*** access the information transmitted prior to the attachment of the EPM.

The EPM is “upstream” of the customer’s access to the information. It is, therefore, integral to the transmission of information, and prior to the recipient’s access to the information.

So even though the USPS has one big customer that uses fax-to-computer as its form of communication, and even though the USPS would like the Commission to believe that this somehow changes the nature of the EPM, the fact remains that the communication between sender and recipient cannot be accomplished until the USPS computers receive a request for an EPM, send that EPM, and retain the record. USPS computers and processes ***intervene between*** the sender’s transmission of and the recipient’s access to the information. It is therefore obviously essential to the communication process. It is in no way analogous to an in-house processing of documents already received, or an in-house process of reception.

The* USPS EPM® *is an Electronic Courier Service, and therefore within the jurisdiction of the Commission, as earlier determined in Docket C99-1.

In 2001, the USPS argued that the complaint in Docket C99-1 should be dismissed as moot because the Postal Service was ending its electronic document delivery business. However, the USPS EPM has resurrected the Electronic Courier Service, PosteCS[6].

When Mr. Foti was asked about a diagram offered by USPS, a diagram that described the USPS's "broader electronic commerce services", he said the following:

Page 197 [7]

> Q. MR BORGERS Very good. On page 11, the last page of this exhibit, this is a presentation made by a Postal Service employee. This actual page came from your responses of your testimony to the OCA. This is just one particular page. Do you think this diagram describes accurately how the USPS postmarking service works?
> A. MR FOTI This diagram is from a presentation which was made over 10 or nearly 10 years ago. I believe the date there says June 1997. This presentation was in the context of a broader electronic commerce service, which at the time the Postal Service was examining.
> Q Okay. So this is not a proper characterization of the current system you have in
> place?
> A No.

In fact, he is wrong. The diagram describes the existing, current document delivery features that are in the USPS EPM today.

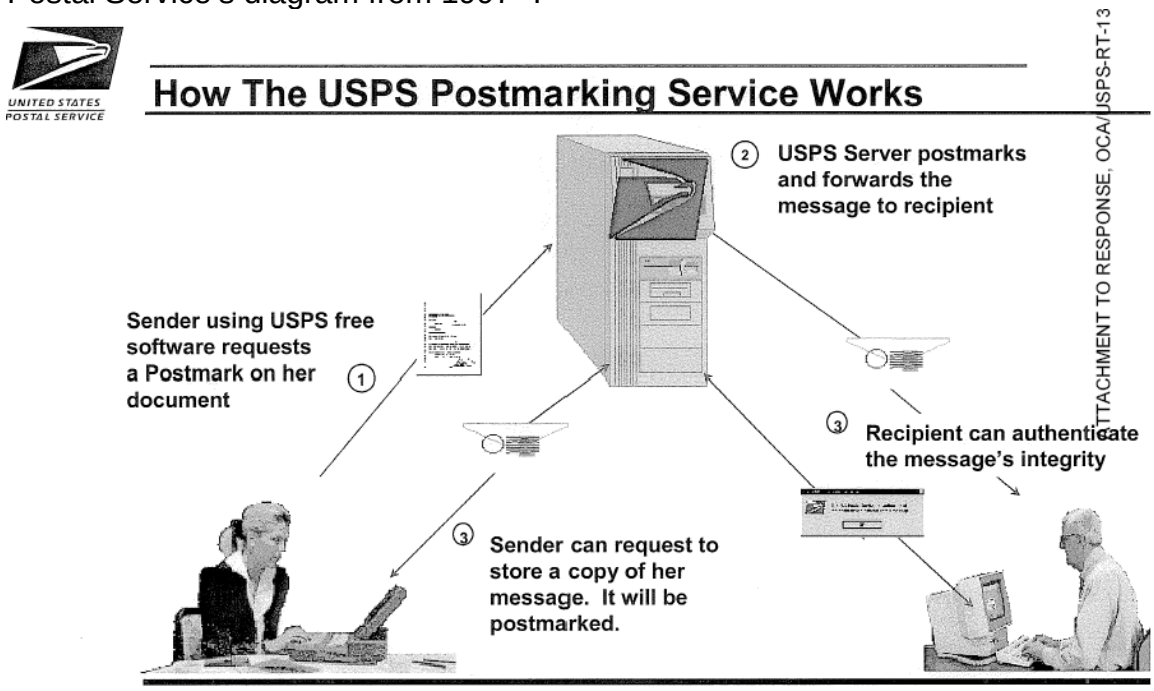
Though this material may seem highly technical, it goes to the heart of whether the EPM resurrects the PosteCS and, therefore, falls clearly within the jurisdiction of the Commission. This 1997 diagram of the broader set of electronic commerce services illustrates how the current EPM works and the function that is available to ordinary customers of the USPS EPM:

---

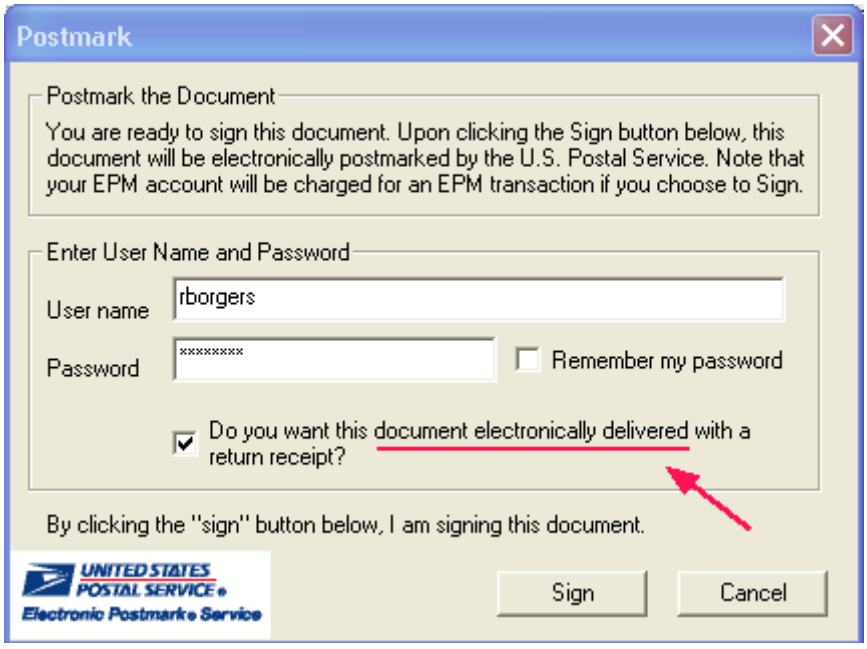
[6] This was also a subject of DigiStamp's *Motion to Notify the Postal Rate Commission of A Recent Example Where the Use of USPS EPM Replaces Traditional Mail Service* on November 11, 2004. The Postal Service did not respond to this motion.

[7] Volume 1 - Official Transcript of the Hearing Held on August 15, 2006

Postal Service's diagram from 1997 [8]:

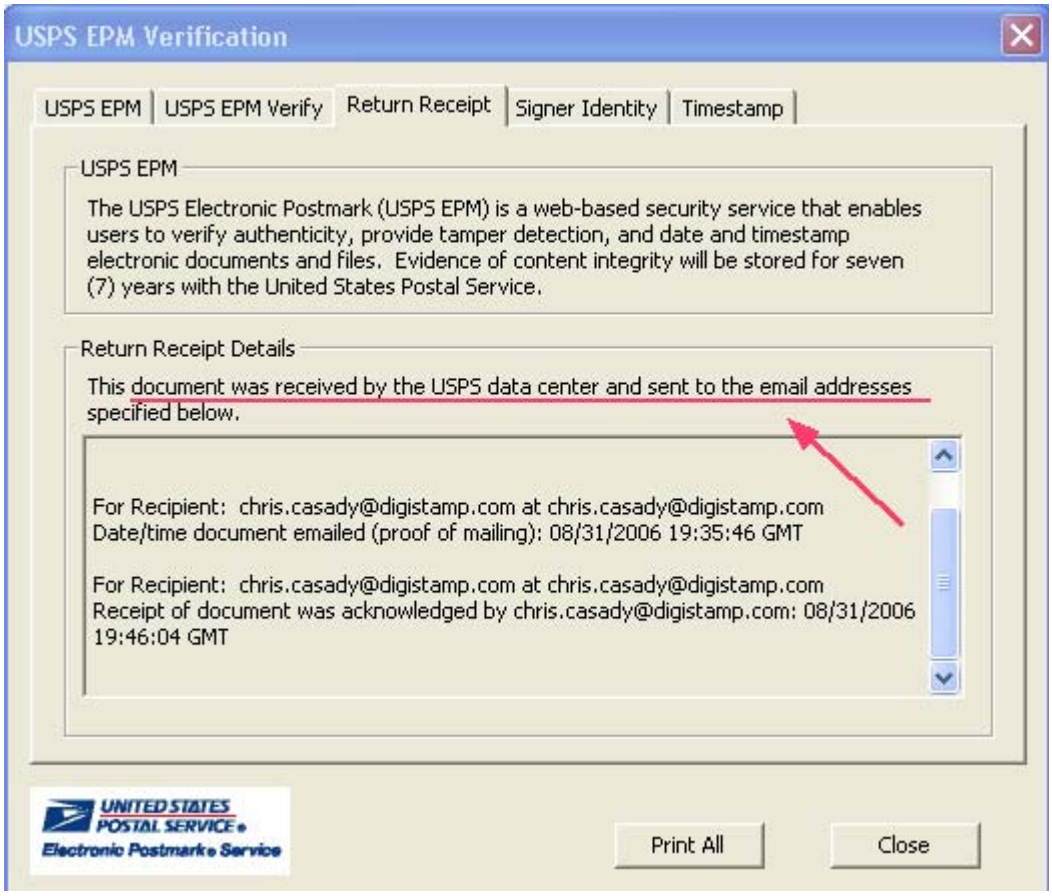


Using the Postal Service's above 1997 diagram, communication of the users document depicted at ① is correct: The user's document is sent to a Postal Service computer. Today's user of the "USPS EPM free software" is presented with this dialog that says it plainly:



[8] United States Postal Service Electronic Commerce Services, June 19, 1997, Leo Campbell, Manager ECS page 3

And at point indicated by ③ in the diagram as getting their proof-of-delivery, the current USPS EPM software says very plainly:



The current EPM contains the function of an Electronic Courier Service, PosteCS. Referring again to the diagram provided by the Postal Service, technically, the communication of data as depicted at ① is correct: The user's document is sent to a Postal Service computer as evidenced by this set of network communications in my examination[9]:

[9] I am supporting my testimony with a highly technical explanation of the communication process. This data is intended for the review by technical staff where they can replicate this test and confirm the results. It is my testimony as a computer system professional that the data presented is accurate and the technique is appropriate to make the factual statements about "what data is flowing where". Shown in the table is the output of a computer network-monitoring program. Using this technique, an investigator can run the USPS EPM software on their computer and monitor all the communications that are occurring. The data collected by the monitoring program is the IP address of the destination computer, the amount of data sent, the actual data sent.

	Sent to as IP address	Protocol	Port	Type	Bytes Sent
1.	63.240.5.40	TCP	443	https	13,103
2.	63.240.5.37	TCP	443	https	2.239,462

The computers at the *IP Address*[10] can be identified by checking the Digital Signature of the SSL certificate that is presented by the computer at that IP address. And in fact, those are USPS computers.

	The "sent to" IP address	Computer Identity[11]	
1.	63.240.5.40	Name = Organization = Organization Unit =	eda.authentidate.com AuthentiDate USPS EPM
2.	63.240.5.37	Name = Organization =	www.uspsepm.com United States Postal Service

By monitoring and varying the size of the document sent, I could confirm that communication to the computer at address 63.240.5.37 includes my document. The content of the document is encrypted using an SSL layer and can be unencrypted / read using the key(s) at the Postal Service's computer.

Referring again to the diagram provided by the Postal Service, technically, the flow of data signified at ② is correct: The user's document is sent as an attachment on an email from a Postal Service computer; this is evidenced by this set of network communications in my examination. Here is the network data about the email's path to the recipient:

[10] An IP address (Internet Protocol address) is a unique number ... Any participating network device — including routers, computers, time-servers, printers, Internet fax machines, and some telephones — must have its own unique address. An IP address can also be thought of as the equivalent of a street address or a phone number or a computer or other network device on the internet. Just as each street address and phone number uniquely identifies a building or telephone, an IP address can uniquely identify a specific computer or other network device on a network. [Excerpt from wikipedia.org]

[11] Computer Identity is confirmed by checking the Digital Signature of the SSL certificate that is presented by the computer at that IP address.

Return-Path: support@uspsepm.com
Received: from mx04.stngva01.us.mxservers.net (204.202.242.98)
by mail19e.g19.rapidsite.net (RS ver 1.0.95vs) with SMTP id 1-0188203001
for <chris.casady@digistamp.com>; Thu, 31 Aug 2006 15:37:13 -0400 (EDT)
Received: from nydb2.authentidate.nyc2.aens.net [63.240.5.41] (EHLO uspsepm.USPSEPM.COM)
by mx04.stngva01.us.mxservers.net (mxl_mta-1.3.8-10p4) with ESMTP id 84a37f44.5172.106.mx04.stngva01.us.mxservers.net;
Thu, 31 Aug 2006 15:36:40 -0400 (EDT)
Received: from nyappl2 ([**63.240.5.37**]) by uspsepm.USPSEPM.COM with Microsoft SMTPSVC(5.0.2195.6713);
Thu, 31 Aug 2006 15:38:29 -0400
Message-ID: <5632870.1157052946541.JavaMail.root@nyappl2>
From: United_States_Postal_Service@uspsepm.com
Reply-To: support@uspsepm.com
To: chris.casady@digistamp.com
Subject: Postmarked Document(s) (USPS EPM Service) from United States Postal Service
Mime-Version: 1.0
Content-Type: **multipart**/mixed;
boundary="----=_Part_485_2377115.1157052946532"
Return-Path: United_States_Postal_Service@uspsepm.com
X-OriginalArrivalTime: 31 Aug 2006 19:38:29.0187 (UTC) FILETIME=[08D67130:01C6CD35]
Date: 31 Aug 2006 15:38:29 -0400
X-Spam: [F=0.2449152541; stat=0.010; spamtraq-heur=0.969(2006083109)]
X-MAIL-FROM: <united_states_postal_service@uspsepm.com>
X-SOURCE-IP: [63.240.5.41]
X-Loop-Detect:1
X-DistLoop-Detect:1
Status:

The originating computer for this email is the address 63.240.5.37 with the Postal Service's computer. This is a multipart email that has the sender's document attached.

Moving forward, referring again to the diagram provided by the Postal Service, technically, the flow of data signified at ③ is correct: A receipt is created and given to the sender from a Postal Service computer; this is evidenced by this set of network communications in my examination. The USPS EPM software on the

sender's computer requests delivery confirmation by getting the *proof of delivery* from the Postal Service's computer.

Sent to as IP address	Protocol	Port	Type	Bytes Sent
63.240.5.36	TCP	443	https	5,140

IP address	Computer Identity[12]	
63.240.5.36	Name = Organization =	www.uspsepm.com United States Postal Service

In summary, the technical data provides evidence of a data flow. The data flow contains a user's document from the Sender to the Postal Service and then from the Postal Service to the Addressee/Receiver. The EPM requires the Addressee to signify that they have accepted delivery before they can view the document[13]. This data flow demonstrates that the EPM includes the function of the Electronic Courier Service PosteCS. Therefore, as an Electronic Courier Service, the EPM falls clearly within the jurisdiction of the Commission.

[12] Computer Identity is confirmed by checking the Digital Signature of the SSL certificate that is presented by the computer at that IP address.
[13] Volume 1 - Official Transcript of the Hearing Held on August 15, 2006, Page 188-189

Appendix A. Clarify the “disputed” fact that a fax is an electronic communication.

1. United States Postal Service 2004 Annual Report Page 20

> Of greatest impact on us are electronic alternatives to business correspondence and transactions, particularly for First-Class Mail items such as bills, statements, and payments. First-Class Mail volumes have already been affected by the telephone, **fax machine**, Internet, and other **electronic communications**.

2. Chief Postal Inspector
http://www.usps.com/postalinspectors/ar03/03artext.htm

> A Message from the Chief Postal Inspector February 2004 I am pleased to present this 2003 Annual Report of Investigations of the United States Postal Inspection Service to our key stakeholders: the United States Postal Service, the Postal Service's Board of Governors, members of Congress, and the American public.
> ...
> The test comprised six modes of **communications**: landline phones, secure telephone units, **fax machines**, the Government Emergency Telecommunications System (GETS), e-mail, and satellite phones.

3. United States Attorneys' Manual Title 9-7.100
http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/7mcrm.htm

> In 1986, Congress amended Title III by enacting the Electronic Communications Privacy Act of 1986. Specifically, Congress added a new category of covered communications, i.e., "electronic communications," which would now be protected, and whose interception would be regulated, by Title III. **Electronic communications** are those types of non-oral or wire communications that occur, inter alia, over computers, digital-display pagers, and facsimile **("fax") machines**. See 18 U.S.C. § 2510(12).

4. U.S. Code TITLE 18 § 2510. Definitions

> (12) “**electronic communication**” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—
>
> (A) any wire or oral communication;
> (B) any communication made through a tone-only paging device;
> (C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

5. U.S. Code TITLE 18 § 1341 and § 1343 Mail and Wire Fraud

Description of Unlawful Conduct - It is a crime to use the mail, private courier, or wire service to conduct a scheme to defraud another of money or property. The term "wire services" includes the use of a telephone, **fax machine** or computer. Each use of a mail or wire service to further fraudulent activities is considered a separate crime. For instance, each fraudulent claim that is submitted electronically to a carrier would be considered a separate violation of the law.

6. U. S. Food and Drug Administration Position on Use of Electronic Communications

We interpret the provisions of 21 CFR §§ 7.49 and 200.5 to allow the use of e-mail and other electronic communication methods, such as fax or text messaging, to accomplish any recall notification or distribution of important safety information. Section 7.49(b) provides that, “A recall communication can be accomplished by telegrams, mailgrams, or first class letters….” Given the use of the term “can,” we read the three examples as being illustrative rather than the sole means of accomplishing recall communications. As explained above, the provisions of 21 CFR § 7.49 for recall communications apply to FDA-regulated products.2 We encourage manufacturers and others to make use of any current technology, including e-mail, to provide information under 21 CFR §§ 7.49 and/or 200.5. We also encourage the use of electronic communications for important safety information not addressed in any FDA regulation, including the communication of voluntary safety information on any FDA-regulated product. We will consider e-mail and other electronic communication methods, such as fax, text messaging or other technological advances, to be appropriate, provided they accomplish the same objective (i.e., effective risk communication) of traditional delivery communications. [from: http://www.fda.gov/oc/guidance/electronic.html]

7. American Bar Association, Standing Committee on Ethics and Professional Responsibility

Formal Opinion No. 99-413 (March 10, 1999). American federal law grants to Internet e-mail and other "**electronic communications**" the same privacy that applies to the Postal Service, commercial mail services, land-line telephone communications and facsimile **("fax") transmissions**. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100

Stat. 1848 (1986), amending this Federal Wiretap Statute, 18 U.S.C.A. Sec. 2510 et seq. (1998). This law provides criminal and civil penalties for the unauthorized interception or disclosure of any wire, oral or electronic communication. 18 U.S.C.A. Sec. 2511. [from http://www.outsourcing-law.com/confidentiality.htm]

8. Authentidate article Move to Electronic Documentation Poses Challenges for HealthCare

Virtually all **electronic communication**, **fax**, e-mails, mailed hard copies, etc. are subject to tampering. Sometimes these changes are obvious, other times they are not. Regardless, unintended changes, errors or omissions can cause significant problems in operations or compliance when the integrity of these documents comes into question. [from http://www.authentidate.com/images/stories/byline_mri_7-2006.pdf]

9. WikiPedia http://en.wikipedia.org

Fax (short for facsimile - from Latin "fac simile", "make similar", i.e. "make a copy" – or telefacsimile) is a telecommunications technology used to transfer copies of documents, especially using affordable devices operating over the telephone network. The words telecopy and telefax are also used as synonyms.