

BEFORE THE
POSTAL REGULATORY COMMISSION
WASHINGTON DC 20268-0001

REVIEW OF NONPOSTAL SERVICES)
)
) Docket No. MC2008-1

**STATEMENT
OF
ADAM GROSSMAN
ON BEHALF OF
EPOSTMARKS, INC.**

Please direct any communications about
this document to:

David M. Levy
SIDLEY AUSTIN LLP
1501 K Street NW
Washington DC 20005
(202) 736-8214
dlevy@sidley.com

Counsel for Epostmarks, Inc.

July 30, 2008

**STATEMENT OF
ADAM GROSSMAN
ON BEHALF OF
EPOSTMARKS, INC.**

I. INTRODUCTION

1. My name is Adam Grossman. I am Founder, President, and Chairman of Epostmarks, Inc., a privately held corporation with offices at 45 Euclid Street, Rochester, New York 14604.

2. As described in more detail below, Epostmarks is a for-profit company that offers an application that uses electronic postmarks within email. My responsibilities for Epostmarks include strategic planning and decision making as well as oversight of all contracts and negotiations. I also established the core infrastructure and operations of Epostmarks.

3. Before working with Epostmarks, I was a project manager in the billing and correspondence IT division of Capital One. The projects under my supervision included initiatives relating to electronic bill payment and presentation.

4. I hold a BS in Industrial and Systems Engineering from Virginia Polytechnic Institute and State University in Blacksburg, Virginia.

5. The purpose of this Statement is to explain, from the perspective of a private sector participant in the Internet, why there is a public need for the USPS-branded version of the electronic postmark, and why this need cannot be met by any private sector participant.

II. DESCRIPTION OF THE ELECTRONIC POSTMARK PLATFORM AND THE APPLICATIONS IT ENABLES THE PRIVATE SECTOR TO DEVELOP

A. Summary

6. The electronic postmark is a flexible technology platform that brings the authority and trust of a national postal operator to electronic transactions. Thomas E. Leavey, Director General of the UPU, has explained that “The service uses the existing assets and trusted brand of postal administrations to bring business into the digital age.”¹

7. In assessing the value of the electronic postmark, it is important to distinguish between the electronic postmark platform and applications that are built to leverage that platform. The Electronic Postmark (EPM[®]) Platform is a standards-based non-repudiation platform designed to accommodate varying applications. While the flexible standard allows for varying operations and configurations, it is a fairly straightforward enabling technology. EPM[®] systems generally do not solve entire problems, but rather enable applications to do so.

8. The Postal Service offers its EPM[®] through authorized service providers. In exchange for a non-exclusive license to offer an EPM[®] with the USPS trademark, the licensed company must: (1) pay the Postal Service quarterly for a minimum number of per-transaction fees, and (2) satisfy certain prescribed quality standards and brand protection covenants. Licensees are permitted to sub-license to application developers that create value-added applications relying on the underlying EPM[®] protocols.

¹ UPU Press Release, *Electronic Postmark Aims to Build Confidence, Trust and Security for Global E-Trade and E-Business* (Dec. 10, 2003) (quoting Thomas E. Leavey, Director General of the UPU).

9. The Postal Service currently licenses the EPM[®] to a single license holder, Authentidate Holding Corp., a publicly traded corporation headquartered in New Jersey.

10. Epostmarks has begun the certification process and is pursuing negotiations to become the second licensee of the Postal Service to provide an EPM[®] system. Our EPM[®] technology complies with the Universal Postal Union (“UPU”) standards and is scalable to perform cost effectively and reliably in all market segments.

B. Electronic Postmark Platform

11. The electronic postmark, also known as a digital postmark, is a content integrity and time-and-date stamp which can be used to verify the authenticity of a document or file sent electronically at a specific point in time.²

12. The first electronic postmark was developed by the USPS and Canada Post in 1998-1999. In November 2003, the UPU adopted technology standard S43 and updated it in 2006. This established an international standard for the interoperability of electronic postmarks across national borders developed by the posts for their own use.³

13. The national postal operators of five countries—Canada, France, Italy, Portugal and the United States—now offer the EPM[®]. Twenty national postal operators—including Sweden, Norway and Denmark—are participating in the UPU

² The electronic postmark offered by the USPS has the brand names Electronic Postmark[®] and EPM[®]. Outside the United States, the electronic postmark is generally referred to as an Electronic Postal Certification Mark (“EPCM”). For the purposes of this statement, I reference all of these collectively as EPM[®].

³ UPU Standard No. S43-3, *Electronic PostMark (EPM) Interface Specification* (approved Nov. 20, 2003).

program of evaluating the potential benefits of establishing an EPM[®] and related electronic services.

14. The components of an electronic postmark are generally regarded as including:

- Digital signature verification;
- Time stamping of successfully verified signatures;
- Stand-alone time stamping;
- Encryption;
- Validation of certificate trust chains; and
- Storage and archival of non-repudiation evidence data needed to verify content and authenticity of an electronic document.⁴

C. Description Of PostmarkedEmail, The EPM[®] Enabled Application Developed By Epostmarks

15. A good example of the value-added applications that EPM[®] enables the private sector to develop and implement is PostmarkedEmail, a value-added application recently developed by Epostmarks. PostmarkedEmail, whose functionality I describe in more detail in Appendix A to this statement, provides guaranteed delivery of messages, proof of delivery, and a trusted icon in the inbox that signals to the user that the email is

⁴ Universal Postal Union, *supra*; UPU Press Release, *Posts and the Information Society: Electronic Postmark Aims To Build Confidence, Trust and Security for Global E-Trade and E-Business* (Dec. 10, 2003); en.wikipedia.org/wiki/Digital_Postmarks (downloaded April 28, 2008).

legitimate and safe to open. PostmarkedEmail also provides proof of sender identity, message integrity, and sender reputation in one integrated solution.⁵

16. Unlike regular email, which virtually anyone can send—and which virtually anyone can fake—PostmarkedEmail is a premium class of email that combines the power of the USPS EPM[®] with user and message authentication technology to create a trusted electronic mail service that protects citizens from online fraud. PostmarkedEmail is sent with a secure, tamper-proof seal and specially labeled – assuring the recipient that an email is authentic.

17. Protecting the email with the USPS Electronic Postmark[®] proves when it was created and when it was delivered. The EPM[®] also adds special legal protections to email, which are enforceable by the U.S. Postal Inspection Service. PostmarkedEmail reduces the risk of ignoring a legitimate email from a bank, online retailer, or non-profit that is real – and the risk of responding to one that is fake.

18. A subscriber to an email address with one of the many other internet service providers that have agreed to recognize the EPM[®], including AOL and Yahoo!, does not need to do anything special to receive PostmarkedEmail; the functionality is built right in. The recipient need only look for the blue ribbon envelope icon in the inbox and the USPS EPM[®] logo in the body of the email. These icons mean the email is real, safe to open, and protected by the USPS EPM[®].

⁵ This statement focuses on the benefits of EPM[®] to the email industry where the Electronic Postmark is especially relevant and Epostmarks has deep domain knowledge. The trust conveyed by the EPM[®], however, is also applicable to many EPM[®] enabled applications leveraged by a growing industry for uses such as document signing, court filings, fax, peer-to-peer, in addition to email.



Figure I: A PostmarkedEmail is real if it contains a blue ribbon envelope in the inbox.



Figure II: PostmarkedEmail messages also include the U.S. Postal Service Electronic Postmark® logo with the familiar “Blue Eagle” icon.

III. THE ELECTRONIC POSTMARK PLATFORM AND APPLICATIONS SERVE IMPORTANT PUBLIC NEEDS.

19. There is an undeniable desire for the trust and protection of the postal service in the digital world. As explained below, in certain markets the need for this trust is dire. These market needs will be met by applications developed by the private sector.

The electronic postmark is the foundational technology that conveys the trust of the Postal Service to application providers.

20. These collaborative roles are important to note, for they leverage the best of what the USPS and private industry each offer. By embracing the international standards, the USPS sets the bar to create a trusted platform with minimal investment of money, time, and other resources. That platform in turn provides an appropriate environment for the private sector to develop applications that efficiently meet market demands for trust products.

21. The availability of multiple licensees of the EPM[®] will assure both continuity of the underlying EPM[®] and competition in the development of value-added applications. Both should encourage continued improvement and faster adoption of the EPM[®]. Additionally, the international nature of the EPM[®] allows U.S. companies to leverage domestic investments abroad in countries with EPM[®] systems.

A. Spam And Email Fraud Have Seriously Degraded The Value Of Email.

22. When email was developed in the 1970s, few predicted how thoroughly it would revolutionize global communications. Today email is one of the most pervasive forms of communication, used increasingly to speed the flow of information and reduce costs. As our dependence on this medium of communications continues to grow, so do business and consumer expectations about what technology can deliver to their inboxes, including security and reliability for high-value communications.

23. The value of email has been degraded in recent years, however, by the explosive proliferation of spam and email fraud. Despite the efforts of both the

government (e.g., enactment of the CAN-SPAM Act) and the private sector, more than 90 percent of all email sent today is some variant of spam. To make matters worse, a large share of spam is not simple advertising, but contains “phishing” messages, purportedly from a legitimate sender, whose purpose is to trick the recipient into disclosing financial account information, Social Security numbers, and other sensitive personal information to the sender of the message.

24. Four aspects of the email ecosystem allow spam and fraudulent e-mail to flourish. First, the anonymity that email senders enjoy makes identifying and catching spammers and phishers virtually impossible. Indeed, most such email today is not sent directly by the wrongdoer’s own servers, but by slave “bots”—computers that, unknown to their owners, have been seized by viruses into sending email at the command of the wrongdoer.

25. Second, the marginal cost of mass-emails is virtually zero. Hence, spam and phishing can be profitable even if the response rate is very low. The result is that fraudsters find it profitable to send millions—or even billions—of illegitimate emails.

26. Third, spam filters, the primary line of inbox defense today, cannot be set to exclude all illegitimate email without also excluding some legitimate email as well. While spam filters have become increasingly sophisticated, so has spam. No permanent victory in the war of spam filters against spam appears in sight.

27. Finally, there is no trusted authority commissioned to regulate and combat abuse of this system. CAN-SPAM and other regulatory laws have been almost entirely ineffective. In 2007, less than *one percent* of spam complied with the requirements of

the CAN-SPAM legislation. Michael Specter, “Damn Spam: The Losing War on Junk Email,” in *The New Yorker* (August 6, 2007) (downloaded from www.newyorker.com on April 27, 2008).

28. Given these factors, it comes as no surprise that spam campaigns have grown tenfold in frequency and scale over the past three years. According to the Anti-Phishing Work Group (“APWG”), over 25,000 unique phishing attacks were reported in December 2007, representing approximately seven million emails per day.

29. Moreover, spoofing—the use of counterfeit websites and logotypes to trick recipients into divulging sensitive account information and passwords—no longer affects just the financial and e-commerce industries. Many other industries now have their brand names hijacked. Approximately 155 popular brands were spoofed in December 2007. See Anti-Phishing Working Group, *Phishing Activity Trends Report for the Month of December 2007* (downloaded from www.antiphishing.org on April 29, 2008). The average consumer received about 80 phishing emails in 2007. Total financial losses were more than \$3.2 billion. Furthermore, online scam artists are increasingly committing fraud by spoofing the identity of the government itself.⁶

B. Industry Responses To Spam And Email Fraud Have Been Costly And Less Than Fully Effective.

30. In response, spam filters have become increasingly restrictive. The effect, however, is that an increasing portion of legitimate and desired emails no longer reach

⁶ ABC News, “Government Warns Public on Fake Emails: Online Scam Artists Increasingly Use Fake Government Emails To Commit Fraud” (July 26, 2007) (available at www.abcnews.go.com/print?id=3418013) (downloaded April 27, 2008).

the recipient. Deliverability is one of the toughest problems facing legitimate senders of email today. Every Internet Service Provider has its own “secret sauce” of white lists, black lists, content filters. The recipes of these spam filters change continuously to combat the continually-changing tactics of spammers and phishers. None of these attempts at calibration are fully effective, however: approximately 20 percent of emails sent by businesses *with the permission of the recipient* are blocked by spam filters. The cost to society from the blockage of legitimate personal correspondence, bank statements, and other business documents is hard to quantify, but undoubtedly very large.

31. Furthermore, because even the most effective spam filters typically allow at least some spam to reach its target, consumers are becoming increasingly wary of email and other electronic services – even those provided by their favorite brands. What do businesses do if their customers refuse to open their emails? Because financial institutions and e-merchants are the most the common targets, phishing activities are degrading trust in the Internet as a preferred tool for business and consumer communications.

C. The EPM[®] Solution Extends To Email The Same Postal Service Model That Has Successfully Maintained Trust In Hard Copy Communications.

32. The USPS has successfully dealt with analogous issues involving hard copy mail. Effective criminal sanctions and enforcement against the disruption of mail service have maintained the public trust even in difficult times. As a result, for over 200 years the USPS has been a critical part of binding the nation together by providing a trusted universal communication infrastructure and continually advancing and improving

message delivery technology. Since the USPS began it has grown and changed with America. The history of the Postal Service is a journey into the history of transportation, economics, industrialization, communications, and government.⁷ And the idea that a citizen can opt to purchase and apply a stamp to written correspondence in return for trusted delivery is intuitive to all Americans.

33. In 2007, the Postal Service was rated one of the ten most trusted organizations in the nation, both public and private. According to the 2007 Roper Poll, the Postal Service was also the most trusted government agency—a ranking that the Postal Service has held for ten years.⁸ On April 7, 2008, the Ponemon Institute found that the Postal Service was ranked first among 74 federal agencies as the agency best able to keep consumer information safe and secure. The Postal Service has increased its privacy trust score every year since the survey began four years ago.⁹

34. EPM[®] extends the same model of trust and economics to email. EPM[®] protected email is a strongly desired class of service missing in today's messaging mix. A trusted class of service including only accredited senders and monitored by the U.S. Postal Inspection Service for criminal activity.

⁷ USPS. (n.d.). *USPS - Postal History*. Retrieved June 20, 2008, from usps.com: <http://www.usps.com/postalhistory/welcome.htm>

⁸ Statement Of Postmaster General/CEO John E. Potter Before The Subcommittee On Federal Financial Management, Government Information, Federal Services, And International Security Of The Committee On Homeland Security And Governmental Affairs, United States Senate, Washington, DC, March 5, 2008 (downloaded from http://www.usps.com/communications/newsroom/testimony/2008/pr08_pmg0305.htm).

⁹ See USPS Press Release, *U.S. Postal Service Again Honored as 'Most Trusted'* (Apr. 7, 2008), avail. at www.usps.com/communications/newsroom/2008/pr08_033.htm (April 29, 2008).

35. A growing number of states have recognized the unique effectiveness of the EPM[®]. For example, since the inception of this proceeding, the Delaware legislature unanimously voted to amend its Uniform Electronic Transactions Act¹⁰. Delaware has joined the ranks of South Carolina, Nebraska, and Maryland in authorizing the use of EPM[®] protected messages as a substitute for First-Class Mail, Certified Mail, or Registered Mail for many purposes.¹¹

D. The Applications Developed By Epostmarks Illustrate The Enormous Value Of The EPM[®] As A Platform For Private Sector Applications.

36. Epostmarks has developed the business relationships, technology, and credibility to provide an application of the EPM[®] in the email market that brings the trust of the mailbox to the Inbox. These relationships depend, however, on continuation of the EPM[®] program by the USPS.

37. Epostmarks' premier relationship with Goodmail Systems provides assured delivery of email messages into the largest ISPs in the country. Some of the carriers that currently accept or will soon accept the PostmarkedEmail token include AOL, AT&T, BellSouth, Comcast, Cox Communications, Road Runner, Time Warner Cable, Verizon and Yahoo!. The monthly volume of PostmarkedEmail messages is nearly 10 million and growing.

¹⁰ See <http://legis.delaware.gov/LIS/LIS144.nsf/vwLegislation/HB+174?Opendocument> (downloaded April 30, 2008).

¹¹ See Maryland Commercial Law Code §§ 21-107(d)(2), 21-118.1; Nebraska Rev. Stat. §§ 86-644; South Carolina Code Ann. §§ 26-6-20(18), 26-6-190(C)(3) and (4), 26-6-195.

38. Several federal agencies—including the Federal Bureau of Investigation, Centers for Disease Control, and Department of Treasury—have begun using the PostmarkedEmail application for their email alerts to the public.

39. Epostmarks also has pilot partnerships in the financial industry (which is poorly supported by existing email technology). A number of financial companies are involved in market testing the Epostmarks application of the EPM[®] platform, and have expressed a strong desire to move forward with the Epostmarks EPM[®] when it obtains USPS certification.

40. A number of other private companies are also taking steps to gain certification from the Postal Service as licensed EPM[®] providers. A conference on EPM[®] sponsored by the Postal Service on January 26, 2007, was well attended by many industry players, including time-stamping companies (Surety, Digistamp, Xyzmo), infrastructure players (IBM, Verisign), and other security companies (Oracle, Adobe, and Wave Communications).

IV. THE PRIVATE SECTOR CANNOT MEET THE PUBLIC NEED FOR THE ELECTRONIC POSTMARK SERVICES PROVIDED BY THE USPS.

41. No adequate substitute for the USPS-licensed EPM[®] is currently available, and no such substitute appears likely to develop in the foreseeable future. No other potential vendor could provide a viable substitute postmark-like service for the EPM[®] from the Postal Service. No software, hardware, or application providers or ISP has the degree of trust of the Postal Service.

42. The fundamental problem is that email authentication is only part of the solution: the sender also needs "reputation." No private sector brand available to the email authentication industry has a level of trust that approaches the trust given to the USPS brand. The only enforceable solution that combines both authentication and reputation in a way that guarantees delivery, and provides reliable proof that the email was delivered, is an EPM[®]-based solution protected by the USPS.

43. Part of the problem is the balkanized structure of the email authentication industry. There are multiple competing reputation providers. And each internet service provider ("ISP") chooses its own reputation provider. Even subscribing to multiple reputation services does not guarantee the delivery of email.

44. Moreover, no other potential vendor has the ability to enforce compliance with its security safeguards through the law enforcement authority of the Office of Inspector General and the Postal Inspection Service. The nonpareil reputation of the Postal Service for information security reflects in large part "the vigilance and effectiveness of the Postal Inspection Service in bringing perpetrators to justice, in serving as a deterrent through their effective investigations, and in participating in education and awareness programs that help consumers protect themselves."¹²

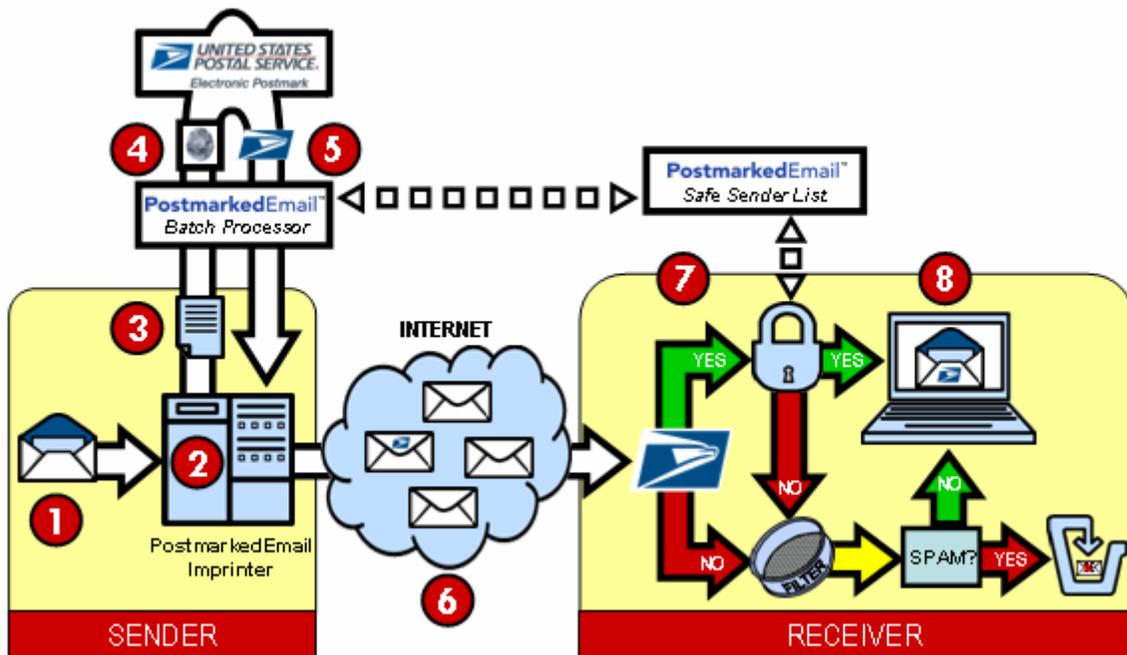
45. For the above reasons, I believe that the Internet will not reach its potential to support a globally competitive United States economy without the EPM[®] provided by the Postal Service.

¹² Statement of John E. Potter, *supra*.

APPENDIX A

TECHNICAL DESCRIPTION OF POSTMARKEDEMAIL

1. The PostmarkedEmail process may be illustrated by the following schematic diagram:



2. In step 1, an email message is created.

3. In step 2, the PostmarkedEmail Imprinter hashes the message to create a unique message digest.

4. In step 3, the message digest is added to an email batch list. A PostmarkedEmail token, including the EPM[®], is embedded in the outgoing email as a visible trust seal and as an invisible signed x-header to prevent tampering.

5. In step 4, the batch list is sent to the PostmarkedEmail Batch Processor where the batch file is sent to the USPS EPM[®].

6. In step 5, a Proof of Creation EPM[®] is issued by the Postal Service and stored by the PostmarkedEmail Batch Processor.

7. In step 6, the email is transported across the Internet using existing standard SMTP channels from the sender to the receiver.

8. In step 7, the receiving email server checks for the presence of a PostmarkedEmail token. If the token is valid the message is placed directly in the recipient's inbox, bypassing all spam and content filters. Proof of delivery information is returned to the PostmarkedEmail Batch Processor by the ISP. A Proof of Delivery EPM[®] is issued by the licensed provider and stored by the PostmarkedEmail Batch Processor for later verification and audit.

9. In step 8, recipients see the email flagged with the blue ribbon envelope in the inbox and with the USPS Blue Eagle in the email, indicating that the email is trusted and safe to open. The technology used is essentially transparent to the recipient, and the recipient does not need any special hardware or software beyond a computer browser with access to the Internet.

VERIFICATION

I, Adam Grossman, declare under penalty of perjury that the foregoing statement is true and correct to the best of my knowledge, information and belief.

A handwritten signature in black ink, appearing to be 'Adam Grossman', is written on a light gray rectangular background. The signature is stylized with a large initial 'A' and a long horizontal stroke extending to the right. Below the signature is a solid black horizontal line.

July 30, 2008