

BEFORE THE
POSTAL REGULATORY COMMISSION
WASHINGTON DC 20268-0001

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

**INITIAL BRIEF OF
EPOSTMARKS, INC.**

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

Counsel for Epostmarks, Inc.

September 10, 2008

TABLE OF CONTENTS

SUMMARY OF ARGUMENT	1
ARGUMENT.....	2
I. THE USPS ELECTRONIC POSTMARK SERVES A STRONG PUBLIC NEED THAT THE PRIVATE SECTOR CANNOT FILL.....	2
A. Description of the USPS Electronic Postmark	2
B. The Governing Legal Standard.....	3
C. The USPS Electronic Postmark Meets A Strong Public Need.	4
D. The Private Sector Cannot Meet The Need For The USPS Electronic Postmark.....	7
II. THE POSTAL SERVICE HAS OFFERED ITS ELECTRONIC POSTMARK SERVICE TO THE PUBLIC SINCE BEFORE JANUARY 1, 2006.....	9
CONCLUSION	11

BEFORE THE
POSTAL REGULATORY COMMISSION
WASHINGTON DC 20268-0001

REVIEW OF NONPOSTAL SERVICES

)
)
)

Docket No. MC2008-1

**INITIAL BRIEF OF
EPOSTMARKS, INC.**

Epostmarks, Inc. respectfully submits its initial brief in this proceeding. Epostmarks is an early stage company, headquartered in Rochester, New York, that offers an application that uses electronic postmarks within email. Epostmarks has begun the certification process and is pursuing negotiations to become the second licensee of the Postal Service to provide an Electronic Postmark (“EPM”) system. Epostmarks’ EPM technology complies with the Universal Postal Union (“UPU”) standards and is scalable to perform cost effectively and reliably in all market segments.

SUMMARY OF ARGUMENT

The Commission should authorize under 39 U.S.C. § 404(e)(3) the continuation of the EPM offered by the Postal Service. The EPM serves a strong public need for more powerful tools against spam, email fraud, and other threats to the trustworthiness of internet communications. The private sector cannot offer a viable substitute for the USPS EPM, for no private firm can match the trusted brand name, enforcement powers, established legal status, and integration into the Universal Postal Union associated with the Postal Service EPM. These facts are confirmed by the broad consensus of support

for the Postal Service EPM by firms ranging from small start-ups like Epostmarks to enormous players like Microsoft.

The USPS EPM properly falls within 39 U.S.C. § 404(e)(3) because the service was offered to the public before January 1, 2006, and has not changed materially since then.

ARGUMENT

I. THE USPS ELECTRONIC POSTMARK SERVES A STRONG PUBLIC NEED THAT THE PRIVATE SECTOR CANNOT FILL.

A. Description of the USPS Electronic Postmark

The Electronic Postmark (“EPM”) is a flexible technology platform that uses the existing assets and trusted brands of national postal administrations like the United States Postal Service to bring business into the digital age. Grossman (Epostmarks) Statement (“Grossman”) ¶ 6. The EPM is a standards-based content integrity and time-and-date stamp, supported and protected by the Postal Service, designed to accommodate varying applications which can be used to verify the authenticity of an electronic file. 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. Grossman ¶¶ 7-14.

A number of EPM enabled applications are already on the market today. AuthentiDate uses the EPM within a medical records management system as well as in a Microsoft Word plug-in used for document signing. The Indiana Bureau of Motor Vehicles uses the EPM to certify driving records admitted as evidence into court proceedings. Epostmarks uses the EPM in its flagship product, PostmarkedEmail, to provide proof of sender identity, message integrity, and sender reputation in one integrated solution. Grossman ¶¶ 15-18.

The collaborative roles of the Postal Service and applications developers leverage the best of what the Postal Service and private industry each offer. The Postal Service sets the bar to create a trusted platform with minimal investment of money, time, and other resources. In turn, that platform provides an appropriate environment for the private sector to develop applications that efficiently meet market demands for trust products. Grossman ¶¶ 19-21, 36-40.

B. The Governing Legal Standard

39 U.S.C. § 404(e)(3) provides that “[n]ot later than 2 years after the date of enactment of the Postal Accountability and Enhancement Act, the Postal Regulatory Commission shall review each nonpostal service offered by the Postal Service on the date of enactment of that Act and determine whether that nonpostal service shall continue, taking into account—(A) the public need for the service; and (B) the ability of the private sector to meet the public need for the service.”

C. The USPS Electronic Postmark Meets A Strong Public Need.

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. Grossman ¶ 22.

The value of email, however, has been seriously degraded in recent years by the explosive proliferation of spam and email fraud. 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. Grossman ¶ 23.

CAN-SPAM and other regulatory laws have been almost entirely ineffective at containing this epidemic. In 2007, less than *one percent* of spam complied with the requirements of the CAN-SPAM legislation. According to the Anti-Phishing Work Group (“APWG”), over 25,000 unique phishing attacks were reported in December 2007 alone, representing approximately seven million emails per day. Grossman at ¶¶ 30-31.

The USPS EPM can defend against spam and email fraud by extending to email the same Postal Service model that has successfully maintained trust in hard copy communications. The model employs two unique assets of the Postal Service: its trusted brand name, and its enforcement powers under federal law. Grossman at ¶¶ 32-35.

To an American, the idea that you can opt to purchase and apply a stamp to written correspondence in return for trusted delivery is intuitive. 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. 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. Grossman at ¶¶ 32-33; Grossman Rebuttal ¶¶ 6.

The public trust in the Postal Service results not only from the history of its service, but also from the effectiveness of the Postal Service's law enforcement authority. Effective criminal sanctions and enforcement against the disruption of mail service have maintained the public trust even in difficult times. Grossman ¶¶ 32. EPM extends the Postal Service's enforcement powers to EPM-protected email. EPM-protected email is a trusted class of service that can be sent only by entities that have been certified for their compliance with the EPM safeguards. This compliance is in turn enforced by the Postal Inspection Service. The federal statutes that empower the Postal Service protect the integrity of the EPM include, *inter alia*, 18 U.S.C. § 1028 (fraud and related activity in connection with identification documents and information); *id.*, § 1029 (fraud and related activity in connection with access devices); *id.*, § 1343 (wire fraud); *id.*, § 2701 (Electronic Communications Privacy Act ("ECPA")); *id.*, § 2510 (regarding electronic communications); *id.*, § 2710 (unlawful access to stored electronic communications). These and other relevant statutes are enforceable by the Office of Inspector General and Postal Inspection Service.

The brand strength and enforcement powers of the Postal Service combine to provide a powerful platform for the development of innovative private sector applications. Numerous companies—from small companies like Epostmarks to enormous market leaders like Microsoft—rely on the USPS EPM for the development of their own applications, or plan to do so once the legal status of the USPS EPM is resolved. Grossman Rebuttal ¶¶ 13-16; Lesur (Microsoft) at 5, lines 15-19; Stamps.com at 4, line 17-18. (supporting “the currently structured EPM program”). Even Digistamp, which asserts that other firms could provide a “time/date stamp” as good as the USPS EPM, concedes that “there is a strong public need for time/date stamp products.” Borgers at 4, lines 1-2.

State governments have also recognized the public value of the USPS EPM. The legislatures of Delaware, Maryland, Nebraska, South Carolina, and Indiana have recognized the unique effectiveness of the EPM by enacting laws and regulations that accord special legal status to Electronically Postmarked files. 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; Haddaway-Riccio Comments (Aug. 26, 2008). As one Maryland legislator has explained, “[M]y constituents need a trusted way to do business electronically and to complete electronic transactions without fear and financial risk. It is my belief that neither USPS nor the private sector alone can meet these needs, however a public private partnership using the USPS EPM can.” Haddaway-Riccio Comments (Aug. 26, 2008). “By USPS providing the EPM and private firms providing the services and application the public has a trusted way to do electronic business.” *Id.*

D. The Private Sector Cannot Meet The Need For The USPS Electronic Postmark.

The EPM provided by the USPS also satisfies 39 U.S.C. § 404(e)(3)(B). The private sector cannot provide many of the key attributes of the USPS EPM, including its trusted brand, the enforcement powers of the USPS, and the integration of the USPS in the established international treaty network of the UPU. Grossman ¶¶ 41-45. Indeed, without the Postal Service's participation, the "fledgling industry segment" of private sector applications based on the EPM "would likely suffer extinction." Grossman Rebuttal at ¶16.

Perhaps most telling are the comments of Microsoft. Microsoft agrees that "The EPM enables the USPS to meet the public need for trusted electronic communication in a way that no private sector organization could rival." Lesur Comments at 5, lines 23-25. That a company with the resources, scale and technological sophistication of Microsoft recognizes the inability of the private sector to offer an adequate substitute for the USPS EPM speaks volumes.

First, no private sector brand available to the email authentication industry has a level of trust that approaches the trust given to the USPS brand." Grossman at ¶ 42. No other software, hardware, or application provider or ISP has the degree of trust of the Postal Service. *Id.* at ¶ 41. Hence, no "other potential vendor could provide a viable substitute postmark-like service for the EPM[®] from the Postal Service." *Id.*

Second, no private sector vendor could match the enforcement authority of the Postal Service, or the vigilance and effectiveness of the Postal Inspection Service as an enforcement mechanism. Grossman at ¶ 44. Even Digistamp, which contends that the

private sector could offer substitutes for the USPS EPM, concedes that a private vendor like Digistamp lacks “the implied legal standing and governmental backing of the USPS, not to mention their sales pitch of federal postal inspectors and special federal laws backing them.” Grossman Rebuttal at ¶ 7 (quoting 2004 Digistamp letter to Congress).

Third, no private sector electronic trust service has the recognized status that the USPS EPM possesses under state law. See Grossman ¶ 35, *supra*.

Fourth, no private firm can achieve the integration of the Postal Service into the Universal Postal Union, a status that is available only to national postal operators. To date, over 100 technical standards have been developed by the UPU. One of those standards, the S43 standard, was “designed by national postal operators for use by national postal operators” and is established to integrate these electronic services into the international postal network. Grossman rebuttal at ¶¶ 22-23. The national postal operators of five countries—Canada, France, Italy, Portugal, and the United States—already offer the EPM. Twenty more national postal operators—including those of Sweden, Norway and Denmark—are participating in the UPU program of evaluating the potential benefits of establishing an EPM[®] and related electronic services. *Id.* at ¶ 13. The USPS and the American public would be at an extreme disadvantage vis-à-vis the national postal authorities of other advanced economies without the capabilities of the USPS EPM and the key industry providers who rely on it. Foti Statement (Jun. 23, 2008) at 3, lines 32-34.

Unsurprisingly, the comments of other parties in this proceeding reveal a broad consensus that the private sector cannot meet the public need for the EPM. See Lesur (Microsoft) Statement, *supra*; Haddaway-Riccio Statement ¶ 2 (“neither USPS nor the

private sector alone can meet these needs, however a public private partnership using the USPS EPM can”).

The lone dissenter is Digistamp witness Borgers. The general thrust of his testimony is that “The private sector not only can meet the need of the public . . . but it is the *only* sector that can do so.” Borgers at 4, ¶ 3. At the same time, however, Mr. Borgers states that “A government agency like the NIST is in a better position to collaborate with industry in the work of setting technology standards/policy and testing the compliance of electronic security applications.” *Id.* 6, ¶ 2. These claims are contradictory—if the private sector is the only sector that can meet the public need, why would they need the help of a public sector organization?

The fundamental error underlying Mr. Borgers’ claims is his misunderstanding of what makes the USPS EPM so valuable and unique. He believes that the critical component of the EPM is its digital time stamp: “I state emphatically that there is a strong public need for time/date stamp products.” Borgers at 4-5; Grossman Rebuttal at ¶ 4. While digital time stamps are undoubtedly important, however, they are not the missing link needed by the public. Time stamps are widely available and easy to implement. The uniquely valuable attributes of the USPS EPM are the trust possessed by the USPS brand and the enforcement powers possessed by the USPS. Digistamp—or any other private sector player—cannot offer those. Grossman Rebuttal at ¶ 6.

II. THE POSTAL SERVICE HAS OFFERED ITS ELECTRONIC POSTMARK SERVICE TO THE PUBLIC SINCE BEFORE JANUARY 1, 2006.

Mr. Borgers contends that the USPS EPM service is ineligible for grandfathering under 39 U.S.C. § 404(e)(3) because the EPM service currently offered by

the USPS differs in fundamental ways from the service offered to the public on or before January 1, 2006. Specifically, he asserts “that the nature of EPM changed fundamentally at the end of July 2007.” Borgers at 3, lines 7-11. Mr. Borgers further concludes that because the EPM currently offered by the USPS was first offered after January 1, 2006, “the Commission has been stripped of the ability to review the nonpostal EPM service.” *Id.* at 3, lines 16-17.

Mr. Borgers’ claim is false. The nature of the EPM has not changed fundamentally since its inception in 1996, a decade before the January 1, 2006 cutoff established by Section 404(e). While the business arrangements maintained by the USPS for participating in the EPM program have changed, neither the ability to meet the public need nor the underlying technology of the service have changed at all. “New business arrangements for the EPM have made it easier for additional partners to participate, but have not fundamentally altered the service for its customers.” Grossman Rebuttal at 9 ¶ 26. As Mr. Grossman explained, “my company can buy the same EPM, with the same account and the same software as in 2005. The only difference is we now do so through a new customer agreement with AuthentiDate instead of with the USPS.” Grossman Rebuttal at 9 ¶ 26.

Even Mr. Borgers has acknowledged at points in his testimony that the EPM service has not changed. On page 23, line 3, of his statement, for example, he claims that “The new business model for EPM involves a branding and licensing agreement, which allows for **continuation of the service without disruption.**” *Id.* at 23, lines 21-23 (emphasis in original). He then goes on to say “The truth is the new EPM program ... needed to approve AuthentiDate simply to *maintain the service operations.*” *Id.* at

23, lines 3-6 (emphasis added). Finally, he summarizes the USPS decision to replace the strategic alliance agreement with a branding and licensing agreement in the following terms: “A more accurate description is that the USPS has *continued the old program with a new method for collecting fees* from the EPM user.” *Id.* at 27, lines 13-14 (emphasis added).

CONCLUSION

For the foregoing reasons, the Commission should find that the USPS EPM serves a significant public need that the private sector cannot fill effectively, and should authorize the Postal Service to continue providing the EPM.

Respectfully submitted,

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

Counsel for Epostmarks, Inc.

September 10, 2008