

BEFORE THE
POSTAL REGULATORY COMMISSION
WASHINGTON DC 20268-0001

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

**COMMENTS OF EPOSTMARKS, INC., ENDORSED BY MICROSOFT CORP, STRIATA, GOODMAIL
SYSTEMS, INC., GOVDELIVERY, INC., AND ICONIX, INC. ON THE VALUE OF ELECTRONIC
POSTMARK PLATFORM AND APPLICATIONS**

Epostmarks, Inc., respectfully submits these comments endorsed by Microsoft Corp., Striata, Goodmail Systems, Inc., GovDelivery, Inc., and Iconix, Inc. to the Commission on the value of the Electronic Postmark[®] (EPM[®]). In the following document we define the EPM technology, its potential, and the value that it can bring to U.S. citizens, businesses, government and the USPS[®]. For the reasons summarized here, we believe that the Postal Service should continue offering the EPM[®].

Introduction

Our nation currently faces significant challenges with email issues that the USPS has successfully dealt with before in hard copy. Vigorous enforcement associated with the security of mail service maintained the public trust even in adverse times. Email needs the trust and assurance that the USPS is uniquely qualified to provide through a public-private partnership¹.

Phishing and spam have wreaked havoc on email communications, and their presence continues to proliferate due to the ineffectiveness of countermeasures in addressing the sheer

¹ For the purposes of this statement we will illustrate benefits of the Electronic Postmarks to the email industry where it is especially relevant. Keep in mind, though, that the trust conveyed by the EPM is applicable to a broad array of digital industries where trusted transactions take place or trusted archiving is important.

volume, sophistication, transnationality, and velocity of duplicitous email activity. The unprecedented growth of fraudulent and unsolicited emails has largely caused a regression in use of email for high value communications and transactions. The capabilities of communications technology have outpaced the capabilities of society to establish and implement appropriate usage standards for reliability, safety, and trust. This leaves U.S. citizens and business vulnerable to situations with dire consequences and no accountability. The USPS can improve convenience of and confidence in the email ecosystem. EPM technology enables the USPS to apply its unique mix of brand power, enforcement, and address verification to help establish sorely needed End to End Trust in electronic transactions.

A Model that Works

For over 200 years, the USPS has played a critical role in binding our nation together by providing a trusted universal communication infrastructure and continually advancing message delivery technology. The USPS has evolved with America. The history of the Postal Service is a journey into the history of transportation, economics, industrialization, communications, and government. (USPS)

The USPS provides a natural model of trust and economics for email that is analogous to the model already established for physical mail. 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.

Benefits to U.S. Economy

More people use the Internet for email than for any other reason, making it the most popular application to emerge from the Internet revolution. Fraud has grown out of control and criminal activity remains undeterred due to lack of accountability on the Internet, which is globally connected, anonymous, untraceable, and rich with targets. The problem today is that those who want greater safety have few effective ways to achieve it. (Charney, 2008) Email is losing the battle and U.S. businesses and citizens are paying their share of the \$60 billion global price tag.

There is a broadly supported technology model called email authentication that, when enhanced by the EPM, can go a long way towards creating a trusted system. In the broadest terms, email authentication allows positive identification of a message's sender. Once a message recipient understands and trusts the identity of a message sender, the recipient can make educated and comfortable trust decisions. Additionally, disclosure of the identity of the sender makes that person or company accountable for its actions.

Benefits to U.S. Postal Service

The EPM positions the USPS as a relevant part of an End to End Trust solution that establishes a foundation for the digital communications architecture of the future. There is strong support for the USPS to fill this role; for example, the Delaware legislature unanimously voted to amend its Uniform Electronic Transactions Act (UETA) in June. They have joined the ranks of South Carolina, Nebraska, and Maryland to provide that EPM[®] protected messages may be used as a substitute for first class, certified, or registered mail under many circumstances. Additionally, the Universal Postal Union, supported by twenty member nations' postal operators, has seen growing interest in and development/implementation of EPM technology. Microsoft has also endorsed the program by cooperating with Poste Italiane in the development of a Microsoft Office 2007 plug-in.

The time is now ripe for the USPS to safely "set the bar" and address the substantial need for trust on the Internet. Beyond keeping USPS competitive on a global scale, this significant role will diversify the Postal Service's revenue stream and maintain the Postal Service's relevance in future online initiatives. By establishing a licensing model (Foti, 2008), USPS has made way for an ecosystem of application developers to efficiently meet market demands for trust products with minimal investment of money, time, and other resources.

Conclusion

The USPS is uniquely positioned to enhance trust on the Internet through the EPM program. Market conditions are optimal with huge fraud problems, broad industry adoption of supportive and complementary technologies, and continued legislative support. By leveraging

existing assets and competencies, U.S. citizens, businesses, government, and the USPS itself will reap huge benefits.

Respectfully submitted,

Adam Grossman
Founder, President and Chairman

Epostmarks, Inc.

45 Euclid St.
Rochester, NY 14604

August 20, 2008

Endorsed By

Garin Toren, Chief Operating Officer

Striata
48 Wall Street
Suite 1100
New York, NY 10005

Striata is an application software developer and service provider focused on enabling electronic billing, interactive marketing and electronic message handling, where key requirements include encryption, document storage and multi-channel delivery.

Daniel Dreyman, President

Goodmail Systems, Inc.
2465 Latham Street
Mountain View, CA 94040

Goodmail Systems makes CertifiedEmail™, the industry standard class of trusted email. CertifiedEmail provides a safe and reliable means for consumers to easily identify authentic messages from legitimate commercial and nonprofit senders.

Scott Burns, CEO

GovDelivery, Inc.
380 Jackson Street
Suite 550
Saint Paul, MN 55101

GovDelivery is the world's leading provider of government-to-citizen communication solutions. GovDelivery's Digital Subscription Management solution is a Software as a Service (SaaS) platform that provides organizations a fully-automated, on-demand public communication system.

Maxim Lesur, Worldwide Postal Industry Managing Director

Microsoft Corporation

**Microsoft Corporation
One Microsoft Way
Redmond, WA, 98052**

Founded in 1975, Microsoft (Nasdaq “MSFT”) is a worldwide leader in software, services and solutions that help people and businesses realize their full potential.

Bill Ames, VP Sales

Iconix, Inc.

**3 2200 Laurelwood Road, Suite A
Santa Clara, CA 9505480**

ICONIX, Inc. is the leading provider of trusted email identification solutions. The Iconix® solution enables consumers to quickly identify messages from legitimate senders, which proactively combats widespread email-based identity theft techniques, such as phishing.

Attachment 1: Technology

The Electronic Postmark (also known as the EPM, Electronic Postal Certification Mark, EPCM, Digital Postmark, or DPM) 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. 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.
- Storage and archival of all evidence data needed verify content, authenticity, delivery, and date and time of delivery of an electronic document.

Attachment 2: Works Cited

Charney, S. (2008). *Establishing End to End Trust*. Redmond, WA: Microsoft.

STATEMENT OF THOMAS J. FOTI ON BEHALF OF THE UNITED STATES POSTAL SERVICE, MC2008-1 (Postal Regulatory Commission 06 23, 2008).

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