



Securing Private Information for Financial Service Providers

Security, Compliance and E-mail

May 2006

Maurene Caplan Grey
Founder, Principal Analyst
Grey Consulting
www.grey-consulting.com

Contents

Executive Summary	1
Financial Service Providers.....	2
Email within the FSP Industry	2
Leveraging Email	2
FSP services	2
NPI transmissions	3
Reach of messaging.....	3
Information Exposure	4
Unsecured email: a hacker’s paradise	4
Securing email: the user’s challenge	4
Legislation and Regulations Breed Ambiguity	5
Gramm-Leach Bliley Act	5
Building an Environment for Compliance	6
Preliminary questions	6
Secure messaging architectures	7
MIT Study on Digitally Signed Email	8
What You Need To Do Now	10
Business and People.....	10
Technology.....	10
Sponsoring Company	11

Figures

Figure 1: Personal Information and Contracting.....	3
Figure 2: Seuring Financial E-Communications	9
Figure 3: Identifying Secured Financial E-Communications	10

Executive Summary

Particularly in the U.S., the financial services industry is heavily scrutinized. Financial service providers are money managers and, as such, have access to the private and sensitive information of their consumer customers. In the act of conducting business, consumer information is transferred to any number of providers. At any link within this chain, security can be breached. Should information like a social security number or credit card number become exposed, the consumer can become the victim of identify fraud.

As a mature communications technology, email often carries the consumer’s private information between financial service providers. However, email is not inherently secure.

To protect the privacy of consumer information, the U.S. government enacted the Gramm-Leach Bliley Act. The Federal Trade Commission has primary responsibility to ensure that financial service providers adhere to the Act.

In response, financial service providers are evaluating methods by which to ensure the security of private information – much of which is transported through email.

Often the exchange of NPI is handled through email messaging.

Email is the common denominator that moves electronic communications.

Financial Service Providers

The Financial Service Providers (FSP) industry is composed of a large number of market sectors, including commercial banking, community banking, retail banking, brokerages, investment banking, payment processing, insurance, reinsurance, mutual funds, credit unions, electronic bill presentation and payment and online banking. Though these sectors represent different types of business services, they each deal with the management of the consumer's money.

To stay competitive, FSP companies are broadening and bundling their service offerings – for example, the “all-in-one” offering. The customer that holds his mortgage, retirement accounts, money market, credit cards and checking account with one provider is likely to get preferential treatment.

FSP companies participate in formal and informal partner communities within which the norm is to electronically exchange a consumer's non-public information (NPI). The communities may be cross-sector and may include the consumer. Often the exchange of NPI is handled through email messaging.

Email within the FSP Industry

Email is a mature transport technology. All commonly used enterprise- and consumer-email backend systems and user desktop and Web clients adhere to Internet email standards.

The consumer is the cornerstone of business across the vast FSP industry, and email messaging is the common denominator that moves electronic communications (e-communications). (Other commonly used types of e-communications include file transfers, instant messaging, print streams, in addition to the as various mediums through which email is delivered.)

Leveraging Email

Companies within the FSP industry have leveraged the near boundless reach of email messaging to deliver new, personalized services.

FSP services

Some of the major categories of such FSP services include:

- Business-to-consumer (B2C) alerts of credit card and banking transactions
- B2C confirmation of financial transactions
- Ad hoc inquiries
- Business-to-business (B2B) electronic invoice presentation and payment
- B2C electronic invoice presentation and payment

Depending on the nature of the business transaction, NPI may be transmitted in the message.

As the breath of FSP services expand, so will the reach of messaging containing NPI.

- Online bill dispute and resolution
- Insurance underwriting and claim management

Personalized services build upon the loyalty of existing customers and arouse the curiosity of potential customers in order to engage them in more profitable and convenient one-to-one relationships.

Yet, personalization requires the exchange of customer information.

NPI transmissions

Depending on the nature of the business transaction, a customer’s sensitive NPI may be transmitted in the message. For example:

- Social security number
- Date of birth
- Account numbers
- Credit rating and credit history
- Acceptance or denial of loan requests

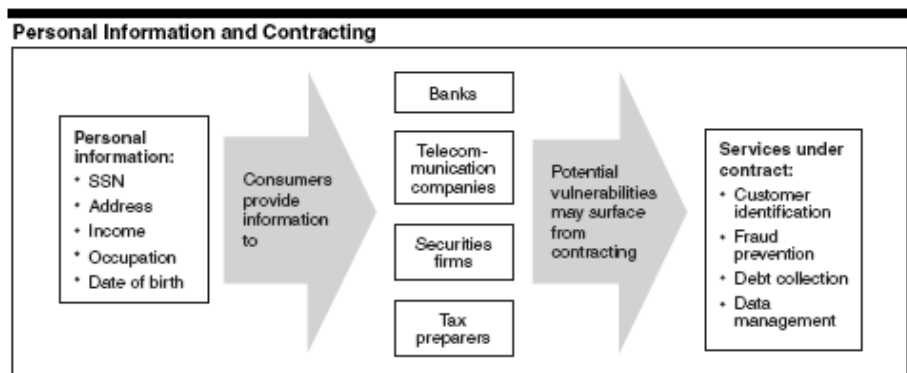
As the breath of services expand, so will the reach of messaging containing NPI.

Reach of messaging

An email message may be sent between members of an Intranet or Extranet community, across the public Internet or a combination thereof.

NPI can be contained in messages sent between traditional financial service providers and external companies – e.g., as contractors.

Figure 1: Personal Information and Contracting



Source: General Accounting Office, January 2006

Anyone can intercept, read, add malicious code, change the message content, change the sender's name and redirect email sent "in the clear."

Information Exposure

Jonathon B. Postel invented the Simple Mail Transport Protocol (SMTP) in 1982. As an early adopter, the Defense Advanced Research Project Agency (DARPA) achieved email security by obscurity. Only select government agencies and universities participated in DARPAnet. Messaging transactions were entered at the UNIX command line.

In 1989, the introduction of the first World Wide Web server and browsers brought the Internet, and SMTP email, to the masses – which led to the demise of email security by obscurity.

Unsecured email: a hacker's paradise

When email messages are sent across the Internet "in the clear," anyone (with the technical ability and inclination) can intercept email, read the message (aka eavesdropping), add malicious code, change the message content, change the sender's name (aka spoofing) and redirect the email. Encrypting email mitigates these risks by providing confidentiality, authentication and non-repudiation. Yet, a majority of users do not understand the importance of encrypting their email messages.

Securing email: the user's challenge

Securing email can be confusing for the user, as well as for the IT security or messaging engineer. Some issues:

- Email systems from different vendors may use different email security protocols, which do not interoperate – e.g., Pretty Good Privacy (PGP), Secure / Multipurpose Internet Mail Extensions (S/MIME) and proprietary solutions.
- Standards-based email security protocols, e.g., PGP or S/MIME, may involve complex key or certificate exchanges in advance of encryption. These keys and certificates may be difficult to obtain and exchange.
- Some email security protocols require additional software to be purchased and installed on both the sending and recipient email clients.
- Incompatibilities between the sender's and recipient's desktop environment may create secure email interoperability issues – for example:
 - The sender and recipient are using the same email security protocol but different versions of the same email client (e.g., Outlook 2000 and 2003)
 - The sender and recipient are using the same email security protocol but different email clients (e.g., Outlook Express and Eudora)

When a message contains a customer's NPI, it is "security-important."

Federal privacy legislation, like the Gramm-Leach Bliley Act, is particularly complex.

- The sender and recipient are using the same email security protocol but different desktop operating systems
- Email messages are transmitted through a variety of means – e.g., desktop clients, Web clients, Web portals, kiosks and mobile wireless devices – many of which do not, by default, have a user interface to easily encrypt/decrypt messages.

Due to a lack of education or experience, the average user does not encrypt their email messages. In practice, the majority of email messages do not need to be secured – an invitation to lunch; a status report; meeting minutes; press releases; product and service announcements; the baby shower for Ellen – important, but not “security-important.”

However when a message contains a customer's NPI, it becomes “security-important,” and must be encrypted to protect both the integrity of the information and the customer's privacy. Privacy legislation in the U.S. and elsewhere has raised the awareness that sensitive information contained in e-mail messages needs to be secured.

Legislation and Regulations Breed Ambiguity

In the U.S., the FSP industry is heavily regulated. Multiple federal agencies may oversee different sections of an Act. Different agencies define their degree of oversight specific to their jurisdiction, or perceived jurisdiction.

Each agency responsible for oversight defines its own diligence level for conducting regulatory audits.

The federal General Accounting Office (GAO) may review how an agency defines its oversight and audit responsibilities.

This structure results in interpretation and enforcement ambiguities, which may never become clear until tested by the Courts.

Federal privacy legislation, like the Gramm-Leach Bliley Act, is particularly complex.

Gramm-Leach Bliley Act

The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act, GLB and GLBA, covers various issues within the financial services sector. Germaine to this paper, the GLBA Safeguards Rule is designed to protect consumer financial information held by a financial institution. The Act defines such data as Nonpublic Personal Information (NPI). Primary oversight of the GLBA is the responsibility of the Federal Trade Commission (FTC). To a lesser degree, seven other agencies hold oversight responsibilities.

As part of a 2004 nationwide compliance sweep, the FTC charged two mortgage companies with noncompliance.

Although email messaging is the primary form of e-communications, print stream, file transfer, IM and P2P applications may also be used.

The Safeguards Rule extends the traditional FSP market to include contractors, subcontracts and vendors that handle consumer NPI. (See “Figure 1: Personal Information and Contracting,” under “Reach of messaging.”)

As part of a 2004 nationwide compliance sweep, the FTC charged two mortgage companies with GLBA Safeguards Rule noncompliance. (See <http://www.ftc.gov/opa/2004/11/ns.htm>.)

Financial service providers generally will be compliant to the best of their ability. Not surprisingly, compliance across the community of FSPs and partners that manage NPI will be spotty at best.

Regardless, protecting NPI builds customer loyalty, and it is the ethical way to conduct business. Additionally, many FSPs have found that secure e-communications open up new, profitable communication channels with customers.

Building an Environment for Compliance

Although email messaging is the primary form of e-communications, print stream, file transfer, instant messaging (IM) and peer-to-peer (P2P) applications may also be used.

Preliminary questions

The following sets of questions can be used as a starting point for assessing your business and technology requirements. These are not inclusive lists.

Business

- What is the sensitivity level of the information being sent? For example, will it need to be secured from the sender’s desktop to the recipient’s desktop?
- Is the NPI contained in B2B transactions? If so, is the other business a trusted business partner with whom you expect to have an ongoing relationship?
- Are you conducting B2C transactions that contain NPI? For example, do your customers log into your Web site to do personal banking?
- Do you use a B2C model for sending credit card statements by email?
- Do any of your customers’ data require specialized handling?
- What type of interfaces (e.g., Web, wireless, etc.) may the sender and recipient be using?

Evaluate different secure messaging architectures. Many enterprises find that a hybrid architecture best fits their needs.

Based upon your preliminary assessment, evaluate different secure messaging architectures.

Technology

- Evaluate email security products based on their capacity to potentially send millions of encrypted e-mails at one time – for example, to support an integrated secure email message center in servicing a number of consumer-facing applications.
- Even if you have decided on a specific delivery method, e.g., a premise-based software solution, ensure that the vendor offers or will be offering multiple delivery models, e.g., software, appliance and managed services. Your business or technology needs may change in the future.
- Evaluate email and document security systems to ensure that they can help your users communicate easily and securely with any of their potential recipients regardless of their skill level and computing environment. This typically requires proprietary technology, in addition to supporting standards-based encryption protocols, e.g., S/MIME and OpenPGP.
- The vendor should support both desktop user-initiated encryption (see “Secure messaging architecture,” “Desktop-Desktop,”) and policy-based, outbound encryption (see “Secure messaging architecture,” “Gateway-Gateway”).
- Regardless of the delivery model, ensure that you can purchase a “baseline” solution and add specialized modules when needed. Ask about bundled offerings.
- When you speak with customer references, ask about the degree to which the vendor has been flexible in meeting non-traditional requirements.
- What methods does the vendor provide for ease of use for the sender and for the recipient?
- Depending on the FSP’s customer needs, is an unusually strong encryption algorithm required?
- What operating systems, application servers, databases and authentication methods does the vendor support?

Secure messaging architectures

Based upon your preliminary assessment, evaluate different secure messaging architectures. Many enterprises find that a hybrid architecture best fits their needs.

Generic names and abstracts are used here. Vendors will use branded names for their own bundled solutions.

The term “message” is used below to mean the email message alone or the message and the attachment(s).

Desktop-to-Desktop. The desktop security software used by the sender will encrypt the message before it is sent. The message stays encrypted on the recipient's computer, until the recipient decrypts the message in order to read it. With a desktop-to-desktop architecture, the encryption software is normally installed as a plug-in to the sender's e-mail client.

Gateway-to-Gateway TLS. "Gateway" refers to the SMTP gateway (aka Mail Relay) sitting at the perimeter (aka edge or boundary) of the email network. The sender's and recipient's SMTP gateways are each pre-configured as secure domains – establishing a trusted connection.

The message is transmitted from the sender's gateway to the recipient's gateway across a secure transport, e.g., Transport Layer Security (TLS). Unlike "desktop-to-desktop," the message itself is not encrypted. However, the transport of the message across the Internet is secured.

Gateway-to-Gateway S/MIME. This architecture is an alternative to Gateway-to-Gateway TLS. The sender's and recipient's SMTP gateways are each pre-configured as secure domains – establishing a trusted connection.

The message is encrypted using S/MIME and transmitted from the sender's gateway to the recipient's gateway, where it is decrypted. Unlike "gateway-to-gateway TLS," the message itself is encrypted – but only between the sender's and recipient's gateways (i.e., not down to the desktop).

Secure Messaging Server. The Secure Messaging Server (aka Staging Server) is often used to transfer very large files between the sender and recipient or for ad hoc messaging, where there is no pre-existing trusted relationship.

The sender's message (and file) is transmitted to the Secure Messaging Server. The server holds the message (and file). The server sends the recipient a notification email message, which includes the URL for retrieving the message (and file).

MIT Study on Digitally Signed Email

In August 2004, doctoral candidates (Simson L. Garfinkel, Jeffrey I. Schiller, Erik Nordlander and Robert C. Miller) at the Massachusetts Institute of Technology (MIT) conducted a survey on the "experience, knowledge and acceptance of digitally signed email." The survey was posted on an Amazon forum frequented by online merchants. The validated survey responses represent the views of U.S. and European merchants. "Views, Reactions and Impact of Digitally-Signed Mail in e-Commerce" analyze the survey results (see http://www.simson.net/ref/2004/fc2005_smime_submitted.pdf).

MIT conducted a survey on the "experience, knowledge and acceptance of digitally signed email."

The degree to which online merchants are covered under the GLBA's definition of FSPs is unclear. Nevertheless, they do handle NPI in the form of credit card information. Survey responses, relevant to this paper, follow.

Figure 2: Securing Financial E-Communications

Table 11. Financial Communications: What Kind of Protection is Necessary?

	“A bank or credit-card statement:”	“Mail to government agencies on official business, such as filing your tax return or filing complaints with regulators:”
Does not need special protection	1.2%	4.2%
Should be <i>digitally-signed</i>	2.1%	9.2%
Should be <i>sealed</i> with encryption	16.2%	9.9%
Should be <i>both</i> signed and sealed	62.7%	64.6%
Should never be sent by email	17.8%	12.2%
<i>sealed or both</i>	78.9%	74.4%
<i>digitally-signed or both</i>	64.8%	73.7%
Total Respondents	426	426
No Response	(7)	(7)

The majority of respondents agreed that e-communications containing sensitive personal information needs to be secured.

Source: Views, Reactions and Impact of Digitally-Signed Mail in e-Commerce (2004)

The majority of respondents agreed that e-communications containing sensitive personal information needs to be secured. However, “Figure 3: Identifying Secured Financial E-Communications” indicates that the majority of respondents are unclear as to what secure messaging means. (Pay particular attention to the responses of the last three questions.)

Figure 3: Identifying Secured Financial E-Communications

Table 3. “What kinds of email have you received? Please check all that apply:”

	ALL	Europe	US
Email that was digitally-signed	22%	33% **	20% **
Email that was sealed with encryption so that only I could read it.	9%	16% *	7% *
Email that was both signed and sealed.	7%	10%	6%
I do not think that I have received messages that were signed or sealed.	37%	30%	39%
I have not received messages that were signed or sealed.	21%	23%	20%
I'm sorry, I don't understand what you mean by "signed," "sealed" and "encrypted".	26%	17% *	28% *
Total Respondents	455	88	367
No Response	(15)	(5)	(9)

p* < .05; *p* < .01;

Source: Views, Reactions and Impact of Digitally-Signed Mail in e-Commerce (2004)

We believe that these results closely represent the views of the average FSP.

What You Need To Do Now

Business and People

- Engage legal counsel to interpret GLBA regulations for your environment.
- Conduct, and reinforce, employee training.
- Educate business partners on your GLBA security and privacy policies.

Technology

- Deploy secure e-mail technologies that fit the relationship model between sender and recipient. Simplicity at the user end is critical for adoption.
- Develop secure e-mail frameworks that are extensible as the FSP community needs evolve.
- Budget for and carry out continuous vulnerability testing and security audits.
- GLBA is designed to protect consumer privacy. Architect security measures accordingly.

GLBA is designed to protect consumer privacy. Architect security measures accordingly.

Sponsoring Company

POSTX

3 Results Way
Cupertino, CA 95014-5924
General Phone: +1 408.861.3500
<http://www.postx.com>

PostX ensures secure encrypted delivery of information vital to business and customer relationships. The company's proprietary technology provides easy-to-use, enterprise-class encrypted communication for regulatory compliance and cost reduction initiatives. Organizations immediately benefit from an increase in effective communications with their employees, partners and customers.

The company is the exclusive secure email provider endorsed by the American Hospital Association (AHA), to provide a standardized secure messaging solution to comply with stringent HIPAA regulations, recommended to the entire AHA network of 37,000 individual health care providers and more than 5,000 hospitals.

The company is headquartered in the U.S. in Cupertino, CA. PostX partners and customers include ABN AMRO, Aetna, Allstate, Aon, BorderWare, Catholic Health Partners, Charles Schwab, Children's Hospital, Citibank, DirecTV Enterprises, eFunds, Groupement des Cartes Bancaires, Hertz, HSBC, IBM, IronPort, Marsh, Mayo Clinic, MessageLabs, Norwich Union, Royal Bank of Scotland, RSA Security, Sendmail, Valero Energy Corporation, United States Postal Service, and Visa.

About Grey Consulting

<http://grey-consulting.com>

<http://grey-consulting.com/blog>

Grey Consulting is an independent research, advisory and consulting firm in the electronic messaging and collaboration markets. With over 20 years of qualitative analytic and "real-world" experience, our analyst staff enables our business and vendor clients to make smart decisions.

Maurene Caplan Grey is the Founder and Principal Analyst of Grey Consulting. Prior to starting an independent firm, Ms. Grey was Gartner's lead analyst on messaging, calendaring/scheduling and human communications. Ms. Grey is a [TMCnet](#) columnist and frequent contributor to [New Communications Review](#), and [MessagingTalk](#).