The Current State of the Industry

Financial firms have moved online to take advantage of the Internet, and have spent billions of dollars on security measures and antivirus software to protect their systems. But when surveying a majority of companies’ security programs, one area continues to come up short—email. To be sure, virtually every company has protection against email-based viruses and spam.

Protection from email is nearly ubiquitous. But what about protection of email?

Today, businesses use email extensively to communicate with their customers and partners, and in that communication, they are including some very important, very private information. But their messages travel across the public internet as protected as a postcard. This practice could facilitate espionage, identity theft, or even full-scale fraud, and leave a company in crisis mode, with some very costly brand repair work for years to come. In addition, sending many types of sensitive customer information via standard email is against the law.

What About Business Processes?

But the issue is not in email alone. Many companies are sharing data with one another over the Internet in a series of automated business processes. An example to consider: John M. turns to the Internet when it comes time to refinance his home. He’s looking for the best rates on his next 5-year ARM. He finds a consolidator that directs him to fill out an online application. In that application, he includes his Social Security number, his address, his employment history, his income, his bank information including balances, and so on. The consolidator then institutes a business process, almost immediately and often automatically farming out John’s request and his information to several partner companies from which John may qualify to receive a loan. And just like that (through that business process), John’s personal data has traversed the Internet in search of a low rate loan. Was the information shared securely? Did the consolidator adhere to government and industry confidentiality and privacy mandates? And if so, was it shared in an efficient manner?

Executing business processes and sharing information over the Internet is essential to businesses and their growth, both in terms of revenue and productivity, and it’s not going to stop. But how can it be done with minimal risk? What can be done to prevent worst-case scenarios? And how can financial institutions weather the storm when they sit square in the eye of the compliance regulation hurricane?

Email and Financial Institutions

According to some industry estimates, as much as 80% of the US population currently uses Internet email. And increasingly—and some might say alarmingly—email is taking the place of postal mail as the preferred form of communication between some of the country’s biggest companies—financial institutions—and their customers. Today, email is a common method of delivering bank statement notifications, mortgage and title information, investment statements and notifications, trade confirmations and other sensitive financial information to consumers. Furthermore, email has become an increasingly popular venue through which financial industry employees can send data and attachments to colleagues for collaboration and review. Workflow (business processes) executed through email empowers the financial industry in new ways and brings new business, increased revenue and increased productivity, all of which, together with cost savings, will further entrench email in the financial industry.

But before it can be used as a universally secure communication tool for sensitive data as well as a
collaboration tool for workflow automation, several potentially significant obstacles must be addressed. This leads to the first question for financial institutions to consider:

### 1. Are we securely communicating with our customers? Does every communication include?

- End-to-end message security
- High-grade encryption
- The ability to send very large documents securely
- Digital fingerprints to verify document originality
- Strong authentication

Email was designed for easy, rapid flow of information, without considering accountability and security of information—essential attributes to the financial industry, especially when sending consumer account information. Private financial records would never be sent on the back of a postcard, yet emailing the same data exposes this information as plain text to the Internet in a similar way.

While sniffing packets constitute the greatest threat while en route, one cannot dismiss what happens at the receiving end of the email chain either. An email message sent over the Internet may be lucky enough to elude interception every step of the way—until it’s received by the intended recipient, who chooses to access the message though a wireless Internet connection that’s not WEP (security) enabled. In this example, the message could even be intercepted by someone as simple as a neighbor piggybacking on the recipient’s wifi. It’s clear that with email transmission there are potential pitfalls at every turn, making true, military-grade encryption essential for any email sent from a financial institution to a customer that contains confidential information or links to confidential information.

In addition to the interception of confidential information while in transmission, there is another question for financial institutions to consider about communications with customers:

### 2. Are our customer outreach programs achieving the best possible response rates?

The Internet is an indispensable tool for companies to communicate their messages and generate new customers. But it’s with existing customers that the real opportunity exists. Customers already familiar with a brand are far more likely to expand their activities with that brand than to go elsewhere, but they must be aware of the many products and services a company has to offer—and the company needs to communicate them regularly enough that, when the customer decides to take advantage of those categories of offerings, either 1) the message has been communicated effectively enough times that the company is already top of mind or 2) the message is received with enough frequency to be in the “right place at the right time.”

For example, John M. is an existing checking and savings account customer of the Bank of North America. If the Bank of North America is effectively communicating their services to John, he knows that they also offer mortgage services, so when it comes time to refinance his house, he knows to go to the bank with which he already does business. Similarly, when he receives his annual bonus from his employer and he decides to purchase a Certificate of Deposit, he knows what the rates are at his existing bank and opts to take advantage of them.
That example of effective communication from a financial institution to its customer results in the most effective form of revenue growth at the lowest cost—increasing the services provided to existing customers. But it’s not as easy as it sounds. Why not? The answer is spam.

Consumers receive anywhere from a handful of spam messages to hundreds of them every day, and they’ve been trained to delete without opening most of them for fear of the malware they may contain. PayPal is a perfect illustration of why consumers don’t open these emails. An enormous number of consumers have PayPal accounts, some of which use them regularly and others almost never, but they all have one thing in common—they receive a frequent bombardment of emails that look as though they’re coming from PayPal and that insist that the customer must click on a link to “update their account information.” Of course these are fraudulent, and as a result, the customer grows weary and fearful of even opening emails that look like they’ve come from PayPal, limiting—and in some cases destroying—the ability of PayPal to communicate with a vast number of their own customers via email. Thus, email has ceased to be as effective a tool for both generating new business and “up selling” to existing clients as it once was (and could still be).

The solution is for companies to communicate securely with their customers and prospects. Businesses must find a way to communicate with their customers in a way that there is no doubt about the true identity of the sender. It must be immediately obvious to the recipient that the email communication is valid and that opening and responding to the email is safe. In short, the secure messaging platform that the business employs must provide the recipient with a sense of security that leaves no doubt, allowing the customer to click on the communication, read it and respond to it, in the process allowing the business to reach their customers—both old and new—with their messages.

The key result a financial institution realizes when it employs a secure mail platform that is trusted by its customers is that response rates have been shown to increase by as much as 10 times, from less than 1% to anywhere between 5% and 10%. This means businesses don’t have to go back to relying solely on postal campaigns—which now cost on average over $1.00 per piece—to communicate their offerings and messages to their customers, and new business generation rates are dramatically improved.

But it’s not just communication with customers and potential customers that must be secured. The flow of information inside the organization must also be considered, leading to the next question:

3. Are we enabling secure business processes within our own organization? When information is received from customers—when, for example, they fill out a web form as in the example above—are we sharing that information securely within our organization?

Above and beyond consumer communication, consider the scenario where John went online looking for a low-rate refinancing option for his home. The amount of personal data we share when applying for a loan is daunting, and the trust we place in the companies to whom we provide that information might be misguided. At times, it makes us think of the good old days…but wait: The old way of paper-based transactions was costly to manage and virtually impossible to automate. Today, the manpower required for handling documents alone could drive a company to bankruptcy. Add to that printing and handling costs, courier costs or postal fees and tracking costs: Productivity plummets and profitability follows. Not to mention the satisfaction ratings in a world of instant gratification when it comes to consumers opening new accounts,
Secure Email and Workflow Automation: Five critical questions every financial institution must ask

having PIN numbers issued and reset, statements delivered, loan applications processed and so on. So, financial institutions must respond to consumer requests and demands securely and with a sense of immediacy, or they risk losing a customer.

Upon receipt of information from a customer, many businesses find it necessary to parse out that information to different work groups within the organization. For example, once John M’s loan application was received, the information had to be parsed and automatically pushed to various departments. One department checked his credit rating and FICA score with all three agencies, another performed a background check for a criminal record, and another verified his employment with his employer. So, John’s personal information was distributed throughout the company, creating yet another opportunity for the unwarranted dissemination of his personal information, and introducing a number of new data loss scenarios.

It is therefore critical that financial institutions adopt an email policy management platform that is configured to identify and automatically encrypt information before it’s sent, or to block the information from being sent altogether depending on a given set of policy-based criteria.

But automated workflow doesn’t happen solely within the organization. Oftentimes, partners are included in this process, which leads to another question:

4. Are we sharing information with our partners so that it arrives securely and automatically—even when they utilize different systems—maximizing revenue growth and improving customer satisfaction?

Today, financial institutions exchange information between one another electronically all the time, and sometimes through automated processes. This is a good thing, if done properly. These processes enable John to receive almost instantaneous bids for his refinance, and result in him receiving the best rates available. In short, it saves John both time and money, and makes him a loyal return customer. So, going back to the old way of doing things is clearly not an option for financial institutions.

If securing internal workflow processes is important, securing external workflow processes is absolutely essential. Once data has left the company network, control is lost, so the time to protect it is before it exits. Many of these workflows are already automated, so the best option is to find a solution that can simply plug into the existing business process between partners to provide protection. Creating a policy platform that can identify and then correctly handle (block, encrypt, etc.) that outgoing information is the best case scenario. If a solution can identify, for example, a Social Security number, it can automatically check to see where that information is headed—to whom at what company. If the intended recipient is authorized, the solution should simply encrypt and send; if not, the information is blocked and the entire process documented.

Another consideration here is the fact that many partners may have disparate systems that can have difficulty communicating directly with one another when it comes to secure email. So the perfect solution would have the ability to enable secure communication without an email platform dependency. This works when the receiving system—different from the sending system—does not have to directly interpret the secure email; it simply needs to receive a notification alerting the recipient that a secure email is waiting. This process would allow the solution to work across heterogeneous mail platforms and still utilize the same email technology already in place and understood by the user, therefore requiring no training. This is significant in that it means the entire investment banking staff of a financial company isn’t required to have IT expertise.
While seemingly simple, workflow automation is perhaps the most important issue for the financial industry to consider today. Managing data as it travels through the various business processes within an organization and eventually outside of that organization is essential to the companies’ continuing success, and workflow automation services can improve the timeliness and reduce the cost of most communications. In addition to that there are both industry and government mandates that lead to the final question:

5. Do we have the auditing, reporting and tracking capabilities in place to meet government and industry compliance mandates and also grow and protect our business?

To illustrate this point, let’s focus on one of the federal acts squarely targeted toward regulating financial organizations:

**The Gramm-Leach-Bliley Act**

Federal legislators are aware of the many limitations of email, and as a result they have passed regulations ensuring the privacy of financial data. The Gramm-Leach-Bliley Act (GLB) mandates the privacy of consumer financial data and it has resulted in sweeping changes in banking transaction and administrative information systems. GLB is quite far reaching, since it defines “financial institution” to be any institution engaged in activities that have been determined to be financial in nature under the Bank Holding Company Act. Though banks are clearly at the core of the legislation, there is no requirement that the company be a bank or be affiliated with a bank. As a result, every time the Federal Reserve and the Treasury determine that an activity is financial in nature and therefore a permissible activity for a financial holding company, a side-effect is that the GLB privacy rules cover a new industry.

Therefore, for financial institutions as well as any business performing activities that are financial in nature, it’s important to implement a solution that meets government mandates and has the auditing and reporting mechanisms required to prove that they are, in fact, being met. The solution must provide the company with the ability to log and refer to various activities over a specified period of time. A tracking capability is a bonus feature here, that should allow companies to know what information was sent to whom, by whom, when it was sent, when it was received and when it was opened.

These mandated customer data security rules often times exceed the capabilities of existing infrastructure services such as email and web portals, and work-around solutions can be labor intensive, expensive to monitor and prone to problems. It’s best to look for a solution that meets these requirements without a complete overhaul of the existing business automation—a solution that simply fits into the existing infrastructure and meets the industry and government mandates, and provides adequate proof that these mandates are being met.

These questions are indicative of the top five issues that financial institutions must take into account today when considering security and their workflow automation infrastructure. It is clear that the ideal scenario would be to maintain the benefits of their existing email systems and automated business processes, expand their use to gain more efficiency and also comply with GLB and other privacy mandates. By
leverages widely adopted open standards for security, and supplementing existing email systems with these standards, this ideal scenario can be attained. One solution that effectively helps companies to address these issues is called DataMotion.

The DataMotion Solution

DataMotion Inc. is a security company that provides secure email for financial organizations and helps them obtain GLB compliance, while securing and streamlining business processes and the sharing of data between organizations. Based on open standards, DataMotion enables financial institutions to rapidly establish secure, accountable, scalable communications with thousands or millions of recipients, including customers, colleagues, and vendors. Once automated the solution requires little human intervention.

With DataMotion, financial employees use their current email client, such as MS-Outlook, Lotus Notes, or even a smartphone like Blackberry or IPhone to send secure email. This eliminates the need for retraining, and results in more rapid adoption by users. Another key feature is ease of use for Internet-based recipients and employees who are traveling or at home, with no special system requirements or software to download.

The DataMotion solution is designed to be easy and ubiquitous, yet offer the high level of security financial institutions need to comply with privacy regulations and mandates. Features such as end-to-end message security, transparent encryption, digital fingerprints to verify document originality and strong authentication provide a very robust security environment. But even with these advanced features, a security system must be easy to use by senders and recipients. By leveraging open standards, using decades of experience in software and security design, and continually learning from customer feedback, the DataMotion system is easy for administrators to manage and maintain, and for users to send, receive and track secure email.

DataMotion Solves Workflow Challenges

DataMotion provides financial institutions with a complete encrypted messaging system offered as a managed (hosted) service or on-premise solution. Customers can use the DataMotion Policy Agent to increase policy compliance, using rules based on email addresses, content, attachment type, attachment size and more. All outbound emails can be monitored for content, key words, numeric strings such as Social Security or bank account numbers, attachments and other information. Once implemented, DataMotion will automatically encrypt, quarantine, drop, copy, log and or block outbound e-mail messages based upon these powerful and flexible rule sets.

DataMotion enables secure workflow (secure business processes) by embedding secure, trackable email into already-existing workflows. And DataMotion goes a step further by providing access to this information through a range of connectors, allowing portals and automated processes to participate in secure communications.

The DataMotion platform accelerates revenue

- Embrace mobile device users running IPhone, IPad, Android and Blackberry, ensuring that they have a first class experience with private communications.
Easily communicate and do business — safely, seamlessly, quickly, and sometimes automatically — with anyone, regardless of their processes, systems, and data formats and in a way that they are already familiar with.

Define when, where, and how to collect, deliver, and receive information for the automation of business processes, allowing companies to do more business with customers and partners — more intelligently, productively, and profitably.

Focus on the opportunities and growth that come from communicating and working with others, not the complexities, costs, and mechanics of doing so.

Comply with government, industry, and corporate regulations through the electronic distribution and tracking of confidential data via email.

Build trust through military-grade encryption and secure connections, built on open standards, to protect both email and other communications in transit so business associates and customers are assured that the information they receive is accurate, timely, trustworthy and secure.

Manage information from small files to very large files up to 2 GB, including automated high-volume transactions traveling through the system.

Enjoy a lower total cost of ownership through a managed service model, available for everyone from the small business to the enterprise.

In conclusion, suffice it to say that communication and workflow challenges in the financial services industry continue to exist today. However, the benefits of doing business over the Internet—whether manually or through automated business processes—far outweigh the alternative of not doing so. Financial institutions therefore must address the issues at hand and look for the best solution to solve these issues. Once the solution is implemented and workflow is secure and automated both inside and outside the organization, real cost benefits can be realized. Add to this the ability to communicate effectively and securely with existing customers and new customer prospects and companies are well on their way to achieving the desired state of security for which they strive and that their customers and partners expect.