SECURING EMAILS IN THE TITLE INDUSTRY

An Introduction to Secure Email Encryption

By ZixCorp
www.zixcorp.com

PROTECTION IS A REQUIREMENT

The October 2015 implementation of the CFPB's integrated mortgage disclosures makes it mandatory for creditors and their agents to safeguard sensitive information such as nonpublic personal information (NPI). In addition to CFPB's regulation, American Land Title Association's Best Practices state that a privacy and information security program should be adopted and maintained to protect NPI. Hence, it is no longer acceptable to conduct unsecure email exchanges with NPI. This is why title and settlement companies are looking for solutions that not only will make them compliant with the new requirements, but also will maintain ease of use for their staff, their partners and, above all, their clients.

SECURITY RISK

Imagine the following scenario. Your client is preparing to send earnest money for an upcoming transaction, so you send an email providing the necessary wire transfer information. Late during the afternoon of the due date you find that the transaction has not yet gone through, and so you call your client to check that they remember to transmit the money. At the other end of the phone you hear silence for a moment before the client informs you - with some passion - that he transferred the money this morning at 9am. After you both talk for a few minutes, the client sends you back your instruction email, containing your logo and your contact details. It is your email, exactly as you sent it, with one exception: your bank account information has been changed. This kind of fraud, known as a man-in-the-middle attack, is expected to increase in the next few years and title agencies and their partners are regarded as soft targets.

INTRODUCING EMAIL ENCRYPTION

Email encryption makes the contents of email, both the text and any attachments, indecipherable to unauthorized individuals. Encryption is used while the emails are in transit, that is, while they are passing through the public Internet, so that if an unauthorized individual intercepts an email while it moves across the Internet it cannot be read. Also, if human error causes a leak where client NPI is sent to the wrong recipient, that recipient will be unable to read the NPI. The greatest benefit of encrypting emails in transit is that the emails are protected while exposed to the Internet.

The beauty of email has always been its ease of use. Unfortunately many email encryption "solutions" force senders and email recipients to use a special key to encrypt and decrypt every single email, thus dramatically slowing down business operations and creating a threat to profitability. Plus the sheer hassle factor for users make such solutions non-viable in most business settings. This complexity and inconvenience has previously prevented the wide spread adoption of email encryption.

In using email encryption, your company can now take advantage of innovative solutions that not only secure email if it's intercepted over the public Internet, but do so without requiring any extra steps from employees, customers and partners. This kind of email encryption solution integrates with your normal workflow. Encryption and decryption happen automatically and invisibly, keeping your business flowing and allowing your company to protect email as it travels outside your network.

Encryption in transit assists title companies in meeting their regulatory obligations. The Gramm-Leach-Bliley Act of 1999 (GLBA) requires institutions dealing with financial information, including title and settlement companies, to handle such financial information "in a safe and secure fashion." Further clarifications by the FTC and the CFPB have made it abundantly clear that financial institutions and their third party providers are 100-percent liable for the loss or compromise of any NPI.

Happily for us, ALTA issued its Title Insurance and Settlement Company Best Practices guide in 2013. This includes recommendations to "[u]se only secure delivery methods when transmitting Non-public Personal Information," and to "[e]nsure secure collection and transmission of Non-public Personal Information." Email encryption fulfills these requirements.

Non-public Personal Information

Personally identifiable data such as information provided by a customer on a form or application, information about a customer's transactions, or any other information about a customer which is otherwise unavailable to the general public. NPI includes first name or first initial and last name coupled with any of the following: Social Security Number, driver's license number, state-issued ID number, credit card number, debit card number, or other financial account numbers.

- American Land Title Association

BALANCING SECURITY WITH YOUR CUSTOMERS' AND PARTNERS' NEEDS

Title insurance and settlement companies who exchange sensitive information with business partners and customers need to secure this NPI while in transit over the public Internet. However they also need to implement this security with minimal disruption to their employees, customers and partners - and to their business operations.

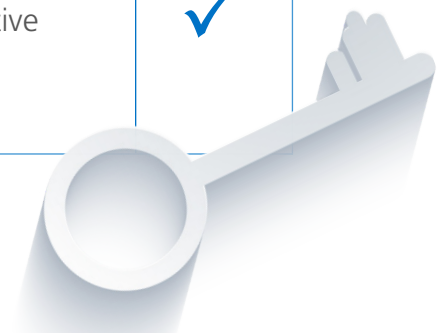
ZixCorp is the recognized leader in email encryption. For example, ZixGateway offers encryption in transit, and is used and trusted by the nation's most influential institutions. With full content scanning of the subject line, message body and attachments, ZixGateway automatically encrypts emails with text or attachments that include NPI. Using state-of-the-art automation and policy-based filtering, ZixGateway removes the risks associated with employee mistakes, relieving them of the burden of deciding when to invoke encryption and enabling them to focus on their primary responsibility – getting work done.

ZixGateway can also remove the hassle and stress for recipients who are your partners and third party providers. When a ZixGateway customer sends encrypted email to another ZixGateway customer, the email and replies are delivered securely and transparently, that is, without extra effort. Of the one million emails encrypted by ZixCorp in a typical business day, 75-percent are sent transparently. And, just in case your recipient isn't a ZixGateway user, we use the Best Method of Delivery (BMOD) to deliver encrypted email in the easiest manner, whether that be ZixMail, transport layer security (TLS) or a secure web portal that can be accessed by anyone, anywhere on any device.

ZixPort is ideal for you to send to and receive emails from end customers, that is, consumers. When you send a secure email to an end customer, they receive an automated email with a one-click link to your own branded portal. It is fast and easy for that customer to create a login so that from then on, you and they can exchange encrypted documents easily; and this includes the customer being able to initiate new communications with you and other members of your staff. With Zix email encryption solutions, title insurance and settlement companies can be confident that they have industry-leading technology that is easy to use for staff and customers, and meets the recommendations for protecting NPI and other sensitive information.

CHECK LIST FOR EMAIL ENCRYPTION

Audit function to demonstrate compliance The audit trail function must work automatically in the background and not require regular management by a member of staff. The compliance reporting user interface should be easy to use and the reports easy to understand.	✓
Large attachments are supported The solution must be able to send emails that contain large attachments. Research shows that without this function, staff will often use alternative means to send large documents, means such as on-line file sharing applications that use the public Internet and are not encrypted.	✓
Policy-based email filtering NPI can be included in the email body or within attachments. The solution must be capable of scanning and filtering through both of these, searching not only for NPI words, but also for patterns associated with personal details and sensitive corporate information.	✓
Easy and intuitive for staff to use The solution should not require more than the most minimal amount of staff training. Using the solution should be virtually identical to what staff members are already familiar with. There should be no extra work effort involved, and staff productivity should be maintained.	✓
Easy and intuitive for end customers The portal for consumers to use should be attractive to the eye and extremely easy to use. It should also make it easy and intuitive for a customer to initiate a secure email exchange without requiring assistance.	✓



zixcorp

ZixCorp is a leader in email data protection. ZixCorp offers industry-leading email encryption, a unique email DLP solution and an innovative email BYOD solution to meet your company's data protection and compliance needs. ZixCorp is trusted by the nation's most influential institutions in healthcare, finance and government for easy to use secure email solutions. For more information, visit www.zixcorp.com.