HUDSON COOK 25th ANNIVERSARY

Encryption Decryption: Breaking Down Email Encryption Requirements Under the Safeguards Rule

By K. Dailey Wilson*

On October 27, 2021, the Federal Trade Commission finalized its long-awaited updates to the Safeguards Rule. The 2021 changes to the rule require financial institutions, including auto dealers and finance companies that offer financing, to dust off their existing information security programs and likely make some significant changes. This article highlights one key change—the requirement to encrypt emails containing customer information.

What is encryption?

As of December 9, 2022, financial institutions will be required to protect by encryption all customer information held or transmitted by the financial institution both in transit over external networks and at rest or to secure such information through effective and equivalent alternative safeguards. Technically speaking, "encryption" means the "transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with cryptographic standards and accompanied by appropriate safeguards for cryptographic key material." I don't know about you, but that definition is about as clear as mud to me, and I am a millennial. In non-IT speak, "encryption" is a process whereby plain text, like a text message or email, is scrambled into an unreadable format. When the intended recipient accesses the message, it is unscrambled and translated back into the original plain text.

What must be encrypted?

When a financial institution sends any customer information through email over an external network, that financial institution will need to encrypt that email. So, what is customer information? "Customer information" means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the financial institution or its affiliates. In layman's terms, "customer information" can include:

- information a consumer provides to you on an application to obtain a credit transaction;
- payment history;
- account balance information;
- the fact that an individual is or has been one of your customers or has obtained a financial product or service from you;
- any information a consumer provides to you or that you or your agent otherwise obtain in connection with collecting or servicing a credit account;
- any information in connection with a financing transaction that you collect through an internet "cookie"; and
- information from a consumer report.

"Customer information" encompasses a lot of types of information that may be included on or in communications you have with your customers. For example, information from the consumer's credit report would be included in an adverse action notice. Account balance information is likely included on monthly statements provided to customers in connection with their motor vehicle financing transactions. If you email these communications to customers, you will now be required to encrypt these emails.

Practical considerations

When implementing an email encryption solution, it is critical to consider the encryption process from the customer's point of view. Encryption solutions that require customers to take additional steps, such as downloading special software to access the encrypted email, could frustrate customers and reduce the likelihood that they take the extra step to actually receive and read important legal disclosures. Accordingly, it is a good idea to test a potential email encryption solution and evaluate its impact on the customer experience before fully implementing it.

Additionally, you should notify both new and existing customers that you use an email encryption solution. Customers who are not expecting to receive an encrypted communication from you may be confused and even concerned that the communication is a phishing attempt rather than an important customer communication.

Finally, note that you could avoid the requirement to encrypt emails by making communications containing customer information available through an alternative method. For example, you could make the information available in a customer's account accessible via username and password (e.g., through an online customer portal), only using email to notify the customer that such communication is available. Because the email would only alert the customer that a notification is available and would not itself contain customer information, email encryption would not be required.

Customers will appreciate the added protection to their nonpublic personal information that an encryption email solution or other equivalent safeguard will provide. Just make sure it's simple to use and not unexpected.

***K. Dailey Wilson** is an associate in the Tennessee office of Hudson Cook, LLP. Dailey can be reached at 423.490.7567 or dwilson@hudco.com.