Wolters Kluwer
Financial Services

INSURANCE COMPLIANCE THOUGHT LEADERSHIP

The Top 5 Things Your Regulator Is Going to Hate about Your Electronic Delivery System

By **Kathy Donovan,** *Senior Insurance Compliance Counsel,* Wolters Kluwer Financial Services

Market Conduct Is Alive and Well, Even in Cyber Space

The regular, rigorous and consistent compliance processes employed by insurers to ensure market conduct compliance in underwriting and claims do not go away in an electronic delivery environment. In fact, insurers using electronic delivery are subject to a plethora of state requirements regulating business in Cyber Space.

Electronic delivery is not a new technology. It is, however, becoming more commonplace among insurers. Insurers have been adding more and more flexibility and options for their customers in the delivery of a multitude of documents and other communications. All of this choice is great for the customer. In fact, this type of customer experience is critical to the bottom line of insurers. But, it opens a new world of security, privacy and market conduct concerns that regulators are starting to notice.

What will this mean for your market conduct examination? Plenty. I have identified five areas of compliance risk exposure that goes hand and hand with electronic delivery. Consider these a sort of checklist – and be forewarned that if you choose to use electronic delivery, your regulator will likely expect that you take care of the following:

1. Pay attention to the types of permitted communications
2. Get consent from your customers
3. Provide compliant disclosures
4. Communicate changes
5. Maintain complete records

1. Permitted communications

Be sure you know what can and cannot be sent electronically, and in which states.

Despite the nearly universal adoption of the Uniform Electronic Transactions Act by the states and the federal E-SIGN Act, insurers still need to verify that electronic delivery for specific transactions is permitted in the individual states. A brief review of Arizona law provides us with examples of transactions which are currently prohibited from being delivered electronically:

- Personal automobile: ARS 20-1632 requires nonrenewal, cancellation or reduction in the limits of liability or coverage notices to be mailed to the named insured by certified mail or USPO certificate of mailing.
- Homeowners: ARS 20-1653 requires all notices of cancellation or nonrenewal to be in writing and mailed to the named insured at the address shown in the policy.
- Commercial lines: ARS 20-1674 and 1676 require notices to be mailed by certified mail to the named insured at the address shown in the policy.

Of course, there are many other notices and other insurance documents which are permitted to be delivered electronically not only in Arizona, but in other states as well. However, it is imperative for insurers to determine exactly what types of transactions and what types of documents are allowed to be electronically delivered. Clearly, this is an issue that is dependent on the types of transactions and documents the insurer is planning to deliver electronically.

Failure to identify and understand the permitted and prohibited electronic transactions at the state, line of business and document level can, and will, result in market conduct violations.

Website Publication of Policy Forms and Endorsements Has Its Own Rules and Risks

A discussion of the compliance risks associated with electronic delivery of insurance documents would not be complete without addressing website publication of policy forms and endorsements. There is a rapidly growing number of states establishing requirements for the posting of property and casualty policy forms and endorsements on insurers' websites. Insurers opting for this electronic "posting" method of forms delivery generally must adhere to specific requirements including declaration page disclosures. It is not uncommon for these disclosures to include:

- that the specimen policy is available on the insurer's Internet website;
- clear identification of each posted specimen policy incorporated into the insured's policy;
- an explanation as to how an insured, on request and at no charge, may obtain a copy of the specimen policy from the insurer; and
- notice of any changes to the forms or endorsements.

Additionally, insurers are expected to provide for these documents' accessibility with requirements such as the specimen policy being:

- easily accessible on the website
- provided in a format readily capable of being saved or printed using a widely available and free computer application or program until such time as no policy incorporating the specimen policy is in force.

2. Consent

It really is all about communication, even in Cyber Space. You must be able to show that the consumer not only desired to have the communication occur electronically, but also that they had the information required to know exactly what receiving that information electronically means. More than just good manners, regulators expect you to be able to document compliant and complete communications… and it all starts with consent.

Looking at this 'first and foremost" step in compliant and complete communications, the insurer is required to obtain the willing consent of the party to engage in, and accept delivery of, electronically delivered insurance documents. Market conduct examiners, in their review of either paper or electronic underwriting and claims files, will verify that there was informed consent of the party. Absent proof of such consent, the examiner could note this failure as a general business practice which is a fineable offense in many jurisdictions.

3. Disclose

You cannot have informed consent without making sure that specific disclosures are provided to the individual in advance —a person needs to understand what he or she is agreeing to and the scope of documents to be delivered. Otherwise, valid informed consent would be lacking, the disclosures would be missing from the insurer's files and the market conduct examination would certainly reveal the communication inadequacy. The specific content of the disclosures can vary from state to state, increasing the potential risk of noncompliance absent current monitoring and implementation of regulatory changes.

4. Notify

Don't forget that your very own operational and infrastructure changes can impact the consent to do business electronically. Ongoing communication must be accomplished in order to notify the consenting parties about changes in hardware and system requirements to permit continued access to electronically delivered documents. Generally, states which have adopted specific electronic delivery requirements require additional disclosures from the insurer if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the individual will not be able to access or retain a subsequent electronic record that was the subject of the consent. The insurer would then be required to provide a statement of such revised hardware and software requirements for access to and retention of the electronic records. Additionally, you must also provide a means for the individual to withdraw consent.

5. Maintain Complete Records

If you can't prove it, it never happened

There is definitely a compelling and absolute need for insurers to prove that the requisite consents were obtained and disclosures given, along with actual tracking of electronic delivery to, and acknowledgment and acceptance by, the addressee. Whether the request for a report for any one or more of these elements comes from an internal compliance auditor, a market conduct examiner, a complaint filed with the DOI or an action filed in court, the ability to track and report on the insurer's electronically delivered communications and documents is a "must-have."

In the event a complaint or an action is filed against the insurer, for example a loss sustained after a compliant notice of policy cancellation was sent, company staff would be best served with a report identifying not only the adverse action notice sent, but also the date/time it was sent and its acceptance by the addressee. Granted, traditional USPS mail or certificate of mailing is sufficiently adequate in many jurisdictions for multiple lines of insurance, but an electronic delivery system with embedded tracking and reporting can provide Legal with more detailed "proof" which can be quite useful in resolving issues efficiently.

Conclusion

Consumers today demand choices, especially in the way that they access information. As insurers continue to innovate and change the way they communicate with consumers to meet those needs, the new communication modes will give rise to new security, privacy and market conduct concerns. Regulators will impose new requirements to protect the consumer and insurers will have to tread carefully to remain compliant. Maintaining an awareness of the states' new and revised provisions is critical so that market conduct concerns are simply that, "concerns" and not violations.

A COMPLIANCE CHECKLIST

- ☐ Does this state permit your transaction to be processed electronically?
- ☐ Did you check for party's consent?
- ☐ Did you check for disclosure, timing and content?
- ☐ Did you verify what the party is consenting to?
- ☐ Did you tell the party how he/she can get a paper copy and what it will cost?
- ☐ Does the state permit you to charge for paper copies?
- ☐ Did you let the party know how they can withdraw their consent?
- ☐ Did you tell the party what hardware and software they need to have to access the documents?
- ☐ Did the party consent in a manner which reasonably demonstrates that he/she can access the documents in the future?
- ☐ Did you notify the party about changes in your hardware and/or software so that accessibility to your documents can be assessed and validated?
- ☐ Do you have a back-up system for paper fulfillment?

Wolters Kluwer
Financial Services

When you have to be right

About Wolters Kluwer Financial Services - Whether complying with regulatory requirements or managing financial transactions, addressing a single key risk, or working toward a holistic enterprise risk management strategy, Wolters Kluwer Financial Services works with more than 15,000 customers worldwide to help them successfully navigate regulatory complexity, optimize risk and financial performance, and manage data to support critical decisions. Wolters Kluwer Financial Services provides risk management, compliance, finance and audit solutions that help financial organizations improve efficiency and effectiveness across their enterprise. With more than 30 offices in 20 countries, the company's prominent brands include: AppOne®, *ARC* Logics®, AuthenticWeb™, Bankers Systems, Capital Changes, CASH Suite™, FRSGlobal, FinArch, GainsKeeper®, NILS®, TeamMate®, Uniform Forms™, and VMP® Mortgage Solutions. Wolters Kluwer Financial Services is part of Wolters Kluwer, a leading global information services and solutions provider with annual revenues of (2013) €3.6 billion ($4.9 billion) and approximately 19,000 employees worldwide. Please visit our website for more information.

Please visit WoltersKluwerFS.com for more information.