Summary Review of Agency Agreements for Technology Content

October, 2014

Table of Contents:

Overview

The ACT Technology Agreements Work Group (Jim Armitage, Chair) put parameters around an updated review of existing Carrier-Agency contracts to determine which emerging or existing technology-related aspects should be inclusive within these agreements. This research built off a previous review published April, 2004.

A total of 18 Agreements were reviewed – These covered carriers from both Personal and Commercial Lines, with an equal scope across national, regional, and super-regional carriers. The Work Group recognizes that not all existing carrier agreements could be reviewed.

For confidentiality purposes, existing Agreements were reviewed only by independent agency employees and association legal representatives.

High-Level Findings

Results show that existing Agency/Carrier agreements fall into the following two primary categories:

- **Combined** Carrier Agency and Technology Agreement. These are positive in that they combine the agency and technology agreements into one document because conflicts can exist between multiple agreements. However, these may be weak overall in being silent on so many important pieces – particularly in respect to agent access to their data after termination.
- **Separate** 'Technology' agreement – Often detailing use of the Carriers' website, and may incorporate Carriers' privacy notice by reference only. Overall, findings on this type of Agreement show:
  - The Agreements tend to be one-sided (accruing to the Carrier's benefit),
  - Do not appear to have any direct relationship with the agency contract,
  - Are not respectful of independent agents' rights and responsibilities, and
  - May violate principles of the agency business.

RECOMMENDATIONS

Based on the Work Group's review, the following are recommendations to carriers when reviewing existing agency agreements and implementing new agency agreements going forward:

Overarching Principles

Intended to detail the primary tenets governing the language and detail of the agreements.

1. Preference for the Technology Agreement is that it should be an addendum to the main agency contract. If for some reason that is not feasible, the Technology Agreement should be a specific, separate section within the overall main Agency Agreement. It is highly recommended that carriers do not create a standalone technology agreement contract separate from the main agency agreement. These recommendations are intended to create the most adaptable environment for future updates, and to provide the clearest and simplest explanation of the technology requirements and obligations of the parties. The Technology Agreements area must also reflect only technology aspects, and not stray into areas of agency/carrier relationship management (indemnification, ownership of expirations, etc.).
2. The agency agreement is and should expressly remain the controlling document.
3. Neither party is allocated responsibility for events for which they have no control. The party found responsible by a court of law, arbitration panel, etc. must accept responsibility for expenses incurred by the other party (indemnification/hold harmless, also as created by third-party), unless payment of such expenses is the obligation of a third party (e.g., an agent's E&O carrier). The language should be constructed that if one party's negligence causes damage to the other party, then the negligent party is responsible for indemnifying and holding harmless the other party to the extent the negligent party caused such damage (i.e., use a comparative negligence standard, and not a contributory negligence standard).
4. Data Retention/Systems of Control (details, timeline, responsibilities, etc.) should be handled in the technology agreement while data ownership and expirations should be addressed in the main agency agreement only. When an agency is terminated, said agency retains access only to **the policies they have issued and endorsed** while in partnership with carrier for as long as they need in order to service their client. The technology agreement should:
    - ☐ Address who is protecting (responsible for) the data.
    - ☐ Distinguish who is responsible for 'data at rest' as well as 'data in transit'. *(Examples: Data At Rest: Resident in the agency management system. Data In Transit: Data being sent from agency to carrier or vice-versa, as in a Real Time workflow.)*
    - ☐ Address which party is responsible for access to data.
    - ☐ Keep Data Protection defined separately from Data Ownership. Data Protection should be addressed in the main Agency Agreement.

Specific Issues to be addressed in Agreements

E-Signatures -

Agreements reviewed were silent on the topic of e-signatures, with the exception of the standard reference of applicable law stating that the contract will be in conformance with all Federal Laws of the United States and specific State Laws, including UETA and E-SIGN. May also take the format that agent shall obtain completed, signed and dated applications for all policies; also they state that all records may be in electronic, not any more specific than that.

Recommendations:

- ☐ If carriers have adopted a formal eSignature policy or have a proprietary system the agents will be using, this must be detailed within the Technology Agreement. This includes minimum requirements

for the agency system use, as well as agency responsibilities for system selection, compliance, and costs. Must meet compliance with E-SIGN and UETA laws.

- ☐ If carriers do not yet have a policy for eSignatures - or if they are in the process of integrating an eSignature solution - the above guidelines for development and inclusion should be used, with specifics detailing the basic characteristics of identity, consent, disclosure, and audit trail.

Click- Through/Clickwrap Agreements -

Definition: An on-screen license agreement that is accepted by the user by clicking a button. Most current software uses the Clickwrap method, which displays the End User License Agreement (EULA) as one of the first screens of the installation program. Example: The installation can be continued if the user clicks "I Agree," "I Accept" or something similar; otherwise the application cannot be installed.

Recommendations:

- ☐ No agreement between agency and carrier should be codified via a click-through agreement, which is typically a one-sided agreement "signed" only by the party against whom the terms are to be enforced. All Carrier/Agency Agreements (including technology agreement addenda) should be accepted and signed by both the agency and carrier via electronic signatures (e.g., using DocuSign, InsureSign, etc.) or traditional 'wet' signatures. In regard to the promotion of technology advancement and ease of doing business, electronic signatures are the recommended solution.
- ☐ Any other references to Click-through or Clickwrap as pertains to customer/agent interaction will be handled in the 'Third-Party' section of these recommendations.

Single Sign-On/Federated IDs –

Definitions:

Single Sign-On: Single sign-on (SSO) systems allow a single user authentication process across multiple IT systems or even organizations. SSO is a subset of federated identity management (ID Federation), as it relates only to authentication and technical interoperability.

Example: One Sign-On and password for all agency systems provided by one unique vendor.

Federated IDs: The means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems.

Example: One ID and password for all agency vendor systems and participating carrier systems as well.

For more information, visit: http://www.signononce.org or http://idfederation.org/.

Many Agreements are silent regarding Single Sign-On on or Federated ID, however some hold agent responsible for restricting access to information only to those persons as is necessary for their job functions.

Recommendations:

- ☐ As the use of Single Sign-On and Federated ID is becoming more prominent, this must be addressed. Agents should encourage their carriers to adopt the industry standard SSO approach.
- ☐ Agreement should address agency responsibility for restricting access to systems only as necessary for agency job functions.
- ☐ Agreement should delineate that an agency representative be responsible for administration of IDs - adhering to industry, carrier, and vendor standards.
- ☐ Note: The ACT Work group recognizes that a key attribute to a successful SSO launch is the importance for agency staff to each have their own individual email address.

Data Breach –

Agreements reviewed reveal addressing this in two primary ways –

INDIRECT: Agreements may not directly address data beach, but the indemnification agreement tends to be a one-sided indemnification, it simply requires that the agent hold the company harmless for any claim, demand, liability, dispute, damage, cost, expense or loss including reasonable attorney's fees and cost of litigation arising out of or in any way connected with your use or access to the carrier's website.
DIRECT: The Agreement states that the agent shall notify the company immediately in the event of any security breach or unauthorized release or use of policyholder's personal info.

Recommendations:

- ☐ Technology Agreements direct that the both parties shall notify the other once they detect and verify any security breach or unauthorized release or use of or access to, policyholder's personal info. Such notice shall include the date and time of such event, the scope and extent of personal info involved and the actions taken by the agent in response to the event. Both parties need to consider that notice requirements for data breaches may include statutory requirements and be very complex.
- ☐ The Technology Agreement should also include a "Hold Harmless' agreement which protects the agent, covering any act or omission concerning the administration of any privacy law. It should also hold the agent harmless for failure of the company to comply with federal or state laws including, but not limited to, the Fair Credit Reporting Act, Federal Truth in Lending Act, Fair Credit Billing Act, and Privacy Law, provided that in the transactions in question the agency use forms supplied or approved by the company. Mutually, it should specifically require that the agent hold the company harmless for any claim, demand, liability, dispute, damage, cost, expense or loss including reasonable attorney's fees and cost of litigation to the extent caused by agency personnel use or access to the carrier's website.
- ☐ Carriers should be indemnified to the extent gross negligence or willful misconduct in using the carrier's agent portal causes damage to the carrier, subject to the agent's E&O coverage.

Prompt Correction to Data and System Errors –
Some Agreements showed a reference to only to agent responsibility, others spoke more directly to removing carrier responsibility.

Recommendations:

- ☐ The Technology Agreement should direct that both the agency and carrier personnel are responsible for prompt correction and notification of data and system errors. *The recommendation is to require that either party notify the other immediately in the event that incorrect information is diagnosed in the system.*

Telematics –
Definition: The technology of sending, receiving and storing information via telecommunication devices in conjunction with affecting control on remote objects. For insurance purposes, often use as a voluntary program given as customer incentive to lower auto insurance rates in exchange for driving behavior data.

Recommendations:

- ☐ As Telematics is an emerging area, the carrier must provide clear education and direction to agents and brokers.
- ☐ If telematics implementation has accessible data, this should be available to the agent/broker for the proper servicing of the client.
- ☐ In the case that a customer calls the agent to inquire about activation/inactivation of a telematics device, the agent should direct the customer to the appropriate supporting technology provider or carrier, as applicable, after which the technology provider or carrier shall be responsible for implementing the customer's request.

Agency Agreement Controlling Document –
Agreements reviewed showed inconsistency in this regard.

Some carrier agreements do not reference the agency agreement as controlling, they create a one-sided indemnity agreement, which states in part that the agency agrees to indemnity etc. for any dispute. There are also no termination procedures detailed.
Other Agreements do provide some clear direction, combining the agency agreement with the technology agreement into one document so there is no appearance of conflicts between the two. The general agreement may also list termination procedures *(Advance notice – Should be at least 180 days)* providing typical termination language. The document also gets into the area of document retention and requires customer files be maintained for 3 years or whatever applicable state and federal law would require. (United Fire)

Recommendations:

- ☐ The Technology Agreements should be an Addendum to the main agency contract in order to be most adaptable for future updates. Must also reflect only technology aspects, and not stray into areas of agency/carrier relationship management (indemnification, ownership of expirations, etc.).
- ☐ Termination procedures should be detailed within the main Agency Agreement. If the Technology Agreement is an addendum, the termination of the tech addendum should be parallel to the main agreement. We look for 180 days minimum notice for contract changes or termination, as this appears to be an emerging standard.
- ☐ If not already covered in the main Agency Agreement, the Technology Agreement should clearly address the agency's electronic use of company logos and signage, as well as agents' duties in licensing and protecting company data and client's data. *Recommendation is that this is handled within the main Agency Agreement.*

Access by Authorized Users –
As with other topics, there was a mix of this being referenced in some Agreements, or merely referenced at a high level in others.

Recommendations:

- ☐ If not already covered in the main Agency Agreement, the Technology Agreement should clearly address the carrier policy ion website access; what constitutes an authorized user, what use of Carrier's property (website, software, etc.) is permitted, and outline the ramifications for unauthorized access or use (e.g., requiring the agency to not misuse or share the user password name that is issued by the Carrier).
- ☐ Agency employees may have access to the carrier's 'Electronic Resources' if the agent grants that authority, however only for business purposes in connection with the sale, solicitation, or servicing of the companies' policies.
- ☐ The agent and all identified users are solely responsible for any misappropriation or misuse, caused by their gross negligence or willful misconduct, of information available on these resources, safeguarding security and confidentiality.

Use of Data by Third Parties –
Most Agreements do not address the use of data by third parties, although some define 'Electronic Resources' as a term.
Definition: Electronic resources refer to those materials or services that require a computer for access, manipulation, or reproduction. Examples: policy data, vendor/state/local databases housing address or property information, also including information available via the internet.

Recommendations:

- ☐ Agreement should require that agent or carrier using third-party data must comply with all applicable laws relating to the user of consumer reports. Must also fully define the term "Electronic Resources".
- ☐ Should mutually define that both the agent and company shall not disclose customer information to any third parties unless the customer has been previously informed of the disclosure, the customer has

authorized the agent or company to do so, and as required or permitted by law or regulation. *NOTE: This provision should be in the main Agency Agreement.*

Click-Through/Clickwrap: Most Agreements reviewed were silent on this topic, however two carriers recommend that the agent audibly read through click-through agreements and this passes ownership on to the third party (customer).

Recommendations:

- ☐ Each carrier Technology Agreement addresses the topic of click-throughs, requiring that agents audibly read through click-through messages to customers as they are presented on-screen, and providing agents with the ability to print out a statement for customers to sign acknowledging that they received this information.
- ☐ Agency principal/leadership must review and understand the intent of agreements before first use by agency staff. In order to achieve this, the carrier needs to obtain click-wrap content and post to a website to make available for agency review.

NOTE: ACT recognizes that there may be contractual or legal limitations on whether or not a carrier or an Agent can share customer data with third parties, and for what purposes those third parties use the data.

Agent Access to Data by Active & Terminated Agency –

Some Agreements reviewed were silent on this aspect; however a number of Agreements reserved the right to terminate agency access to carrier systems without notice at their sole discretion. It is understood that language is intended to protect the insurer in the event of some sort of outage over which it has no control.

Recommendations:

- ☐ Agreement should detail clear parameters for cancelling agency access to carrier systems.
- ☐ Providing the agency/brokerage continues to service the customer, the carrier should either transfer all applicable policyholder data to the agency within 1 year, or allow agency access to the carrier policy system until the agency transfers all applicable policyholder data to itself or a third party designated by the agency (not to exceed 7 years). This information may be crucial for the agency if it faces an E&O claim or lawsuit which can arise up to 6 years after the subject insurance was procured. If the agreement provides for a shorter period of time than 7 years for the agency to access the customer information and then extract what is needed, the agreement must clearly specify how long the agency will have the ability to do this.
- ☐ For best service to the customer, access should also include not only the actual policy in place with all of its endorsements, but the full activity log for that policy.
- ☐ The agency for its part must take necessary data transfer action in an expedient manner, as appropriate for the agency's circumstances.