

ACT 2019Oct23 Meeting – API Breakout Notes

Discussion Leader: Duke Williams

1. What components should we address?

- a. Key security areas to provide guidance
 - i. Physical systems
 - ii. Development operations
 - iii. User access
 - iv. At-rest and In-motion encryption – acceptable security communication level/algorithm
 - v. Password management
 - vi. How to collaborate with a reputable vendor/consultant
 - vii. Creation of a business agreement (BAA)
 - viii. Check user agreements for PII requirements
 - ix. GDPR/NY DFS/ California CCPA
 - x. Overall, how to authenticate vendors using security standards as they apply to APIs
- b. Determine: Are agents the weak link in security? If so, how do we help mitigate this?
- c. Challenge: Agents do not have control over API development, but the big players do, and determine security levels/protocols
- d. Provide guidance to agents with more homegrown apps – Ensure they understand the perils of insecure use of APIs.
- e. Top critical business areas & transactions APIs can solve:
 - i. Interconnectivity with carriers
 - ii. Quoting & Sales
 - iii. Policy Management
 - iv. Claims Management
 - v. Alerts & Notifications
 - vi. Billing
 - vii. Real Time; mobile apps, 3rd-party apps
 - viii. Marketing info/Sellsheets
 - ix. Telematics and integrated data shared with agents.
- f. Critical need: True TWO-WAY communication, not just positive capabilities
- g. What is preventing you from engaging in vendor and carrier API discussions?:
 - i. They can't execute (yet) on what we want
 - ii. Systems limitations
 - iii. Multiple systems (and resulting complexity)
 - iv. Complex effort to expose APIs – Must tie into all systems
 - v. Agents & Vendors might not know who to talk to at any given carrier.
 - vi. Prioritization within AMS development for vendors.
 - vii. Many competitors

ACT 2019Oct23 Meeting – API Breakout Notes

- viii. Cost is not the main issue, but a clear ROI is not there in every case to develop an API. **NEED:** Helping to determine whether there is truly a business requirement which necessitates an API (primarily because existing products do not meet the need).
- ix. Potential liabilities with non-public information
- h. Management system vendors should approve every API vendor they work with in ALL cases.

2. To what depth is useful?

- a. This will depend upon each audience – Agent/Low-Tech, vs. Agent/Hi-Tech, Carrier, Vendor)

3. What format for guidance is most useful to you/your company?

- a. A guide to how the API can create growth for the agency
 - a. Time savings
 - b. Remove non-revenue-generating tasks
 - c. Simplification of processes.
- b. Provide agents with a list of of questions. Examples:
 - a. Where is my data stored?
 - b. In motion/At rest – US vs Canada
 - c. What is the security policy of the API provider?
 - d. What is the audit process and data governance?
- c. What are things you can and cannot do with an API?
- d. Standards and Guiding Principles. Use a common language all can understand and move forward with.
- e. A 'Top 10' Things to Ask an API Tech.
- f. This is more a full-industry initiative, but a Developer Toolkit would be very useful, as there is a lack of standardized datasets.

+++++