How Embedded Compliance Plays the Game to Win, Not Break Even

By Greg Bierl, Vice President of Revenue and Counsel at Compliance Systems.
This article was originally published on BankDirector.com, September 23, 2021.

Imagine a game where your team can't score points and there's no such thing as winning. All you can do is meticulously follow the rules; if you follow them well enough, then your team doesn't lose. Most banks approach compliance with this survival mindset and it shows.

According to the Federal Reserve Bank of St. Louis, **compliance expenses account for 7% of banks' non-interest expenses**. The majority of that spend is typically directed at headcount distributed across siloed operational functions — using equally siloed technology — to get the job done during the last leg of a transaction. The best that can be said for this approach is that it achieves baseline compliance. The worst? It prevents institutions from investing in transaction data management strategies that deliver compliance while simultaneously driving efficiencies and business growth that show up on the bottom line. This scenario becomes more untenable with each passing year: Increasing compliance complexity drives up costs, and that diversion of investment erodes a bank's ability to compete.

Banks can choose to play the game differently, by viewing compliance as an integrated part of the data management process. Solutions that leverage application programming interfaces, or APIs, provide a mechanism for technology components to communicate with each other and exchange data payloads. Outside of this approach, transaction data resides in bifurcated systems and requires extra handling, either by software or human intervention, to complete a transaction and book the right data to the core. Having the same data in multiple systems and rekeying data dramatically increase an institution's risk profile. Why make it harder to "not lose" the game when banks can leverage API-first solutions to ensure that data is only collected once and passes through to the touchpoints where it's needed? **The key to unlocking this efficiency is a compliance architecture that separates the tech stack from the compliance stack.** Otherwise, banks are obliged to wait for code changes every time compliance updates are pushed.

Mobile enablement is now as critical for a bank's success as any product it offers. The customers that banks are trying to reach have no practical limit to their financial services options and are increasingly comfortable with contact-free experiences. According to studies from J.D. Power & Associates released this year, 67% of U.S. bank retail customers have used their bank's mobile app and 41% of bank customers are digital-only customers. Given historical trends, those numbers are expected to only increase.

Compliance represents an opportunity to remove friction from the mobile banking experience, whether offered through an app or a website. Traditional PDF documents are designed for in-branch delivery and are a clumsy fit for the mobile world. Responsive design applies to compliance content no less than it applies to mobile apps; content needs to adjust smoothly to fit the size of the viewing

screen. The concept of “document package” is evolving to the point where a “compliance package” should be constructed on responsive design principles and require minimal user clicks to view and acknowledge the content.

An embedded compliance solution should treat optimized mobile channels as table stakes. To survive and thrive in this environment, institutions need to be where their customers are, when they are there. Traditional banker’s hours have officially gone the way of the dodo.

Embedded compliance can also enhance bank data security in the event of a breach. It is difficult to overstate the reputational damage that results from a data breach. Embedded compliance offers critical safeguards for sensitive customer information, bolstering an institution’s overall security profile. Legacy compliance or document-prep solutions often require duplicate data entry and expose customer personal identifiable information to the inherent data breach risks that come with multiple databases scattered across technology platforms. Look for solutions that do not store PII data, and instead offer bi-directional integrations with your platform.

Increasing demand for digital engagement provides banks with opportunities to rethink their technology stacks. Management should evaluate each component for its potential to address a myriad of business needs. Compliance solutions can sharpen or dull a bank’s competitive edge and should be considered part of a strategic plan to grow business. Who knows, maybe someday compliance will actually become “cool”? A dreamer can dream.

1575 Arboretum Drive SE, Suite 406 • Grand Rapids, MI 49546
www.compliancesystems.com | TEL 800.968.8522