Flyer

opentext™

The Paradox of Personalized Financial Services

In the competitive financial services market, delivering a personalized user experience is mission-critical. In doing so, service providers own all the responsibility of protecting customer data and ensuring responsible business conduct. This makes comprehensive compliance archiving and supervision strategies vital.

The State of Service Customers' Experience

An analysis of the financial services industry released by Salesforce in November 2020 revealed two striking insights about the state of service customers' experience.[1] First, 68 percent of customers said that COVID-19 had raised their expectations of service providers' digital capabilities. Second, only 27 percent expressed the opinion that the financial services industry is customer-centric. Further, an even smaller fraction—23 percent—said that they believe the industry handled the pandemic well.

Where do financial service providers fall short, according to survey respondents? The study pointed first and foremost to customer experience (CX), which respondents rank with the same level of importance as a firm's product and service offerings. As a corollary, the study found that respondents expect their providers to understand the unique needs and expectations of each of their customers.

Better Personalization through Digital Enablement

Not surprisingly, the key enablers for personalization will be digital technologies. The customer experience once depended on personal relationships built over years through branch office conversations with well-trained account managers and advisors. Customers now demand convenience and transactional immediacy. Yet they refuse to sacrifice personalized services—investment and strategy recommendations, or the ability to consult with experts while opening or modifying accounts, for example—for this convenience.

To meet customers' growing demand for personalization, financial service providers have turned to digital technologies, including offering live chat options on web sites or apps, chatbots on transaction pages, and new forms of convenience enabled by partnering with third-party social collaboration vendors.

Of course, the digitization of financial services can also bring new efficiency and scale to service providers' business operations, in addition to satisfying customer needs for the personal touch.

As customers volunteer personal data in exchange for a more tailored and meaningful experience (as they used to when working with an account manager or investment advisor), service providers can glean insights to inform new product development, strategic innovation, and competitive differentiation. Plus, as

---

1 *Salesforce News & Insights, "Lessons from Nearly 2,800 Financial Services Leaders on Resilience in the Face of Crisis."*

customers grow to rely on their financial firms, they develop a sense of trust that drives increased brand loyalty and faster adoption of new services to meet their evolving needs.

Increased Responsibility and Risk in Managing Personal Data

Within this fabric of interdependency lies the paradox of personalized financial services. Service customers demand ever-higher levels of personalization from their service providers. Financial service providers turn to digital technologies to personalize the CX efficiently and at scale.[2]

By asking customers for information to help guide investment decisions, service providers and customers enter into a mutually beneficial trust relationship. To sustain and nurture this relationship, service providers bear virtually all of the responsibility for protecting and preserving this customer data.

It's important to note that extracting value from this data—both for customers and for the business—usually involves moving it from its point of collection. Organizations need to aggregate the data centrally before processing it to identify patterns and trends. They need to correlate it with account information in their Customer Relationship Management (CRM) systems, as well as with other market and demographic data.

Service provider employees often need to import or ingest data into more specialized systems for more detailed analysis, reporting, or presentation. They can automate the flow of this data for routine processing and analysis, and thereby protect it from inappropriate handling or exposure. But process exceptions happen, especially for high-growth financial service trailblazers. These exceptions—often simple process workarounds improvised by employees under deadline pressure—can put the company at risk for compliance violations, litigation, and crippling reputation damage.

Compliance Archiving and Supervision: Obligations and Opportunities

Financial service providers face a growing list of regulations to collect, retain, and preserve electronic communication data to maintain legal business conduct. In this regard, archiving and supervision are often considered necessary burdens, a cost of doing business in the highly regulated financial services sector. Yet financial service startups can also view archiving and supervision as another tool for innovation. As they experiment with different ways to meet their customers where they live, and query the data these customers share, employees will inevitably stumble. An employee blunder may risk exposing customer data, sharing insider information, committing an act of collusion, or worse. The act may be calculated or may be completely innocent.

Given the enormous obligation service providers have to police employee behavior, an effective archive is mission-critical for monitoring day-to-day communications and taking necessary corrective measures. To manage legal or regulatory challenges when they arise, service providers need an archive engineered for rapid search and context-rich analysis. These solution attributes are essential for conducting early case assessment (ECA), determining the firm's likely success in litigation.

To proactively monitor employee communications and conduct, financial service providers need AI-powered supervision and surveillance capabilities. Supervision allows compliance officers to run periodic samples of employee communications data to spot potential acts of fraud, insider trading, collusion, or other illicit or inappropriate behaviors. AI technologies integrated into supervision systems enable continuous improvements in accurately and effectively detecting red-flag events.

Conclusion

Consumers and institutional investors alike increasingly choose their financial service providers based on the personalization features of their user experiences. Service provider upstarts need to innovate constantly to improve their reach, operational efficiency, and scale.

To serve both sets of needs, financial service providers rely upon a variety of interactive software technologies and approaches to foster dynamic, trust-based relationships with their customers. These relationships demand that service providers assume extraordinary responsibility for managing customer data securely and transparently.

Compliance archiving and supervision solutions are mission-critical for enabling this level of stewardship over customer data. Implementing archiving and supervision solutions that deliver intuitive operation, high performance, simplified pricing, and comprehensive support for increasingly diversified communication data types (i.e., generated by email and a growing array of social collaboration tools, e.g., Salesforce Chatter, Microsoft Teams, LinkedIn, Twitter), are table-stakes requirements in any financial service provider's growth strategy.

Learn more at
www.microfocus.com/foundations
www.microfocus.com/opentext

Connect with Us
OpenText CEO Mark Barrenechea's blog

2 *The Financial Brand, "The Future of Customer Experience in Banking is Personalized."*