Thomson Reuters CLEAR

Trends in digital banking

5 digital financial services trends that are shaking up the industry

Learn where the future of finance is headed — and the importance of streamlining digital operations and modernizing risk management.

If a modern-day Rip Van Winkle were to nod off now for a 20-year nap, the changes he would witness upon wakening would be mind-boggling. Emerging technologies such as DNA storage, quantum computing, and automated vehicles are just some innovations on the horizon that might soon have all of us scratching our heads. And modern-day financial services professionals may soon be feeling a similar sense of bewilderment about changes in their industry, even without tuning out for a decades-long nap. The ongoing global digital transformation will continue to impact the financial services industry mightily — an acceleration of change that has already dramatically altered the industry in just the past few years.

And significant changes are sure to continue: In a recent survey, 66% of financial services executives said they believe that new technologies will continue to affect and reshape financial services in the next five years. More than 40% are concerned about regulation of data protection and similar digital technology and how it might impact their organization's bottom line.

Because these trends shape the roles of those on the front end of the financial services industry, they are worth watching and understanding. It is wise to prepare for those changes now, not only to enhance your own performance, but also to improve the customer experience and productivity for your business.

Here is a look at five of the biggest areas of innovation in the financial services industry, as well as recommendations for how to prepare your organization to tackle them.

THOMSON REUTERS®

1. Cryptocurrency

The first form of decentralized cryptocurrency, Bitcoin, appeared in 2009 with a value of less than one penny. Today, one Bitcoin is worth tens of thousands of dollars. Many other forms of cryptocurrencies have appeared in the years since Bitcoin's introduction, and the total global value of the cryptocurrency market is in the range of $2 trillion.

Cryptocurrencies are founded on a form of database technology called blockchain. As often happens with new technologies, there has been some resistance to the acceptance of cryptocurrencies. A survey of financial services professionals found that 63% believe cryptocurrency to be a risk, with criminal activity such as hacking and fraud being their main concerns. China, for example, has outright banned bitcoin trading.

Nevertheless, many traditional financial services organizations will be compelled to embrace cryptocurrencies just to stay competitive, thanks to increasing consumer demand. According to another survey, ***more than 22% of U.S. adults own bitcoin***. The same survey found that four out of five bitcoin holders would move their cryptocurrency funds to a bank if secure bitcoin storage were offered as a service.

The lack of U.S. regulatory oversight of the cryptocurrency industry has been one factor impeding the acceptance of cryptocurrency by the traditional financial services industry. But recent and forthcoming regulations, such as the Anti-Money Laundering Act of 2020 (AMLA 2020), may soon mandate increased governmental regulation of the cryptocurrency industry. In sum, it's likely that traditional financial services organizations will face increasing pressure to become much more involved in cryptocurrencies in the next few years, and governments will be scrambling to enact regulatory legislation. The imbalanced regulatory state, with some countries taking a harder line than others, also may shift the balance of power for cryptocurrency companies and users. This is particularly pertinent for financial organizations with an international presence.

Criminal activity in this sector is also worth watching. Fraud and hacking top the list of crimes that federal and state authorities fear the crypto financial services industry may be vulnerable to. In August 2021, the PolyNetwork crypto platform was breached, with $600 million of its customers' assets temporarily falling into the hands of hackers. And in September 2021, OFAC sanctioned Suex OTC, a Russia-based virtual cryptocurrency exchange, for moving hundreds of millions of dollars in cryptocurrency gained through illicit and high-risk sources.

2. Decentralized finance

Cryptocurrency has enabled another trend that may profoundly affect the financial services industry: decentralized finance (DeFi). Examples of DeFi platforms include Maker, a decentralized lending platform, and Compound, a decentralized money market protocol. DeFi platforms offer all the services that traditional financial services organizations offer without the need of an intermediary, with blockchain technology and computer code replacing the traditional role of the bank. The DeFi financial model allows anyone to have access to financial products and services online in a decentralized and borderless environment. In some ways, DeFi has the potential to eliminate the need for traditional banks.

> "In roughly an 18-month period corresponding with the emergence of DeFi, around $80 billion of capital has been transferred to DeFi platforms — and each dollar represents funds diverted from the traditional financial services system.

As DeFi gains traction and increasingly competes with the services provided by traditional financial organizations, the industry will likely need to embrace and, to a degree, adopt DeFi methodologies as evolutionary innovations. More efficient and streamlined internal processes and compliance workflows will be key to morphing DeFi from an existential threat to an opportunity for these organizations.

3. Anti-money laundering

Money laundering has long been a concern for the financial services industry. Since the enactment of the Bank Secrecy Act of 1970 (BSA), financial services organizations have been responsible for helping to monitor and report activities that may be associated with money laundering. But just as technology has expanded the toolset that criminals can access for laundering money, so has technology armed financial services organizations with an array of sophisticated "weapons" for detecting and reporting money laundering activities.

For several years, government has urged financial services providers to be more proactive in deploying the tools of modern technology in the fight against money laundering. In 2018, several government agencies, including the Federal Reserve and the FDIC, issued a joint statement promoting the adoption of technology in identifying and reporting money laundering: "The agencies recognize that private sector innovation, including new ways of using existing tools or adopting new technologies, can help banks identify and report money laundering, terrorist financing, and other illicit financial activity by enhancing the effectiveness and efficiency of banks' BSA/AML compliance programs. To assist banks in this effort, the agencies are committed to continued engagement with the private sector and other interested parties."

In 2020, Congress passed AMLA 2020, which is designed to strengthen and expand anti-money laundering laws while encouraging the use of technology in maintaining compliance with those laws. In essence, AMLA 2020 expanded the 1970 BSA act by subjecting the financial services industry to significantly broadened regulatory compliance and enforcement actions, along with enhanced penalties for compliance violations. Simultaneously, the 2020 Act encourages the use of technology in detecting and reporting illicit financial activities. The act mandates that each financial regulatory agency appoint an innovation officer charged with providing awareness and

guidance in adopting technological innovations in anti-money laundering. The intent is to help financial services organizations make sense of digital trends and comply with the Bank Secrecy Act (BSA). For compliance officers and anti-money-laundering professionals, it may provide their employers the push they need to modernize practices. AMLA 2020 also directs the U.S. Treasury Financial Crimes Enforcement Network (FinCEN) to brief Congress periodically on relevant emerging technologies.

The impact of this legislation on financial services organizations is hard to understate. A 2018 General Accounting Office study of 11 banks found that direct costs associated with BSA compliance ranged as high as $21 million for a single financial services organization. And non-compliance with anti-money laundering rules can be even more costly, from a financial and reputational perspective. Capital One, for example, was fined $390 million in early 2021 for anti-money laundering violations spanning multiple years.

Financial services professionals bear the brunt of the burden in assuring compliance with anti-money laundering regulations. The good news is that technology can significantly ease that burden. Simply shifting searches from a manual process to an automated process, for example, can eliminate the many false positives that expand workloads and diminish accuracy.

4. Financial services regulations

For highly regulated industries such as financial services, changing technologies can spur the need for new or restructured regulations that reflect the realities of the modern, digitalized environment.

There is a significant gap between current financial services regulations and the digital world in which financial services providers must operate — a world that's expected to be impacted by more technological changes in the next few years, further broadening the gap between regulations and reality. Regulation often is reactionary, as evidenced by the Dodd-Frank Wall Street Reform and Consumer Protection Act in 2010. Although the impact of that legislation is still a large piece of the reality for many in the financial services industry, from its enhanced checks and balances to its emphasis on creating a physical paper trail, it came after the financial crisis that closed more than 450 U.S. banks. Rules cannot go back in time and fix the problems that preceded them. They are also slow to change on their own, as evidenced by the challenges that financial workers have found with adhering to physical documentation practices in a remote work environment. This puts the onus on financial services organizations to address issues on their own, even as the rules behind them become a moving target.

Regulating agencies such as the Federal Deposit Insurance Corp. and the Office of the Comptroller of the Currency are already at work digitizing the regulatory process to keep up with technological advances in finance. This will drive the financial services organizations themselves to enhance their own digital capabilities with a move toward automation, so that their processes and employees can stay aligned with this changing regulatory scene.

5. Data and digital analytics

Technological advances have enabled the generation and storage of vast quantities of data. And the rate of accumulation and the diverse array of sources is continuing to accelerate:

> "Between 2010 to 2020, the amount of data created and stored worldwide increased by nearly 5,000%.

In the next three years, the amount of data that will be collected is projected to exceed the total amount of data collected over the previous 30 years.

This presents an opportunity and a challenge for the financial services industry. Data is most valuable when it is usable and accessible. For financial services providers, digital analytics is a means of maximizing the value of data, harnessing it for providing greater insights into customers and the processes that serve them.

With the aid of artificial intelligence and machine learning, digital analytics can power basic financial services operations with greater efficiency and accuracy. Data analytics already is an essential part of front-end workers' daily duties in managing customer relationships and protecting the financial services organization from bad actors. The use of automation in identification verification and fraud detection is imperative for flagging and managing risk in an increasingly digital and wide-ranging environment. But, as with all trends, it also represents a two-edged sword.

Organizations that seek to leverage the benefits of digital analytics to solve real problems are likely to profit greatly. Conversely, financial services organizations that fail to embrace or properly use digital analytics may soon find their ability to onboard and serve customers severely diminished. The competitive landscape for financial services already includes players such as Google, Amazon, and similar tech companies for whom data analysis and digital best practices are commonplace. Staying relevant and keeping financial services organizations secure now requires playing on the same field as digital-native organizations.

How to prepare your organization to stay ahead of the curve

Meeting the significant challenges of these trends will occupy the attention of every financial services organization in the next several years, if it doesn't already. A common thread running through the five trends is technology — and technology is the solution that will help traditional financial services providers prepare to meet those challenges. Here are a handful of recommendations for using technology to prepare your organization for the future:

- **Replace manual processes with automation to streamline internal workflows.** Many financial services organizations remain mired in manual processes that simply can't provide the speed and accuracy that are so essential to remaining competitive in the digital age. With automated technology, you can keep up with evolving customer expectations driven by fintech competitors, as well as innovations such as cryptocurrency and DeFi.

"Automation is less about removing roles or jobs and more about gaining speed and accuracy in critical processes, which can allow people to innovate and react quickly.

- **Use tech tools to reduce risk.** Whether you're onboarding new customers or considering new investment instruments, technology and automation can help by sleuthing out potentially risky customers and third parties. For example, a sophisticated investigative platform can give you:
  - Fast and accurate real-time identification verification for customer onboarding, including remote identity authentication
  - Risk verification and alerting
  - Identity theft detection and alerting

  In addition to keeping your business secure in the long term, these capabilities can help you quickly and accurately verify the identity of a business or individual investor — so you can be sure, for example, who really owns the cryptocurrency you are considering.
- **Leverage technology to ease the burden of anti-money laundering and regulatory compliance.** Automated anti-money laundering technology can significantly ease the burden of BSA and AMLA 2020 compliance for financial services organizations. As regulators become increasingly digitized, building your own digital capabilities can help your organization stay ahead of the changes to come.
- **Use analytics to bring out the value of your data.** Of all the advantages of technology, perhaps the most valuable is its ability to make data usable. The success of Fintechs at leveraging their data to win customers away from traditional financial services has made digital transformation an imperative for these organizations.

For financial services organizations of all sizes, technology provides the answer for surviving and thriving in a world significantly changed by technology. And for organizations that have been doing a bit of virtual napping as evolving technologies leave them behind, it's time for a wake-up call.

Thomson Reuters® CLEAR offers financial services organizations a single-solution intelligence platform that helps reduce risk from fraud, alerts to negative media incidents, and streamlines customer onboarding. Discover how your organization can better serve customers, enhance employee productivity, and manage the challenges and trends of the digital age with CLEAR.

THOMSON REUTERS®