FUTURE-FORWARD COMPLIANCE

Unleashing Efficiency for Streamlined Success in the Digital-Native Future
The bank compliance function stands on the brink of fundamental change driven by digital technology. This transformation has already begun and is likely to accelerate sharply as generative AI drives new thinking about both the compliance challenges and the compliance solutions of the future.

Generative AI tools like ChatGPT are sparking both hopes and fears across most spheres of business. On the one hand, there is trepidation. The ability of these AIs to manipulate language has stoked concerns that they could help bad actors spread misinformation or profit from fraudulent scams. On the other hand, entities in government and the private sector increasingly embrace the technological renaissance, eyeing smarter data tools and digital-native systems to reduce costs and improve back-office efficiency.

For bank compliance professionals, lightning-fast technology innovations—particularly AI-powered tools to analyze enormous amounts of data—present new risks but also opportunities. The head of the Federal Trade Commission, Linda Khan, recently told Congress that AI technology such as ChatGPT could “turbocharge” fraud.¹ AI has already been used to mimic pop musicians in fake songs placed on (and then removed from) streaming services.² In May, an AI-created photo purporting to show an explosion at the Pentagon briefly moved the stock market.³ In financial services, one can imagine criminals using AI to invent identities, fake loan documentation, and use increasingly creative means to trick unwitting bank officers or consumers.⁴
A Future with Better Outcomes
At the same time, many businesses are rushing to update their technology infrastructures to serve a variety of purposes. Some regulators are urging financial institutions to address outdated IT to reduce errors and improve efficiency. A recent report by the U.S. Chamber of Commerce said small businesses use an average of three technology platforms to power their operations. According to the survey, about a quarter of the technology resources used by small businesses are for fraud prevention. Even law enforcement agencies have signaled that corporations suspected of wrongdoing could face tougher prosecutions if their compliance programs lack data analysis technology.

These developments foreshadow marked changes in bank compliance functions over the coming years. By as early as 2030, regulatory monitoring for financial institutions of all sizes will likely rest on a digital-native architecture, with the capability to process data more quickly, analyze it more effectively, and more readily and accurately identify red flags. These compliance systems will require new skill sets but also have the potential to drastically improve results. Changes in the industry will likely also be accompanied by innovation among the regulators themselves to track industry activity more effectively by supplanting their analog-based, legacy infrastructure with a more digital-native technology platform. Some regulators are already urging financial institutions to address outdated IT to reduce errors and improve efficiency.

The purpose of this article is to explore what is possible in the development of digital-native compliance programs. One benefit of adopting regulatory technology (regtech) in banks’ compliance programs—mirrored by adoption of supervisory technology (suptech) at the agencies—will be lower operating costs. This cost restructuring, in turn, can help to level the playing field for small banks that today incur disproportionately high operating expenses, including for their compliance programs. Other benefits will include improved outcomes in monitoring for money-laundering, identifying fair-lending gaps, allowing for alternative underwriting data and more.

Understanding the Varied Compliance Cost Landscape
Compliance costs are one of the highest noninterest-related expenses incurred by financial institutions. A 2020 global survey of 245 senior executives found that approximately a third of financial institutions spend more than five percent of their revenue on compliance. Compliance costs are obviously highest for the largest banks that employ large internal departments of legal, compliance and risk management teams. However, compliance demands are in some respects heavier for smaller community banks with a higher amount of regulatory demand relative to their size. They cannot afford to operate large in-house compliance departments, nor to outsource substantial work to outside lawyers and consultants. The same is true for technology platforms. Large banks spearhead much of their own digital innovation from within, while community banks rely on a handful of core processors that manage the technology stacks for thousands of banks. Similarly, small banks have cost disadvantages in relation to fintech firms, which generally have highly efficient digital-native and cloud-native compliance technology, with none of the legacy infrastructure that makes small-bank operations expensive to manage.

Continued growth in regtech solutions over the next five to ten years will give community banks in particular greater options to address their compliance needs with more precision and lower costs, thereby helping to level the playing field between large and small institutions. Regtech tools powered by AI and faster processing speeds can help institutions automate the monitoring of anti-money-laundering (AML) threats, pore through massive amounts of data identifying fair-lending risk and use alternative credit data in their underwriting systems, among other purposes. A 2021 study by Juniper Research found that regtech spending by banks and other heavily regulated companies to satisfy compliance requirements for customer onboarding is projected to exceed $130 billion in 2025, nearly quadrupling the spending in 2020. The research focused on how regtech can benefit digital onboarding and compliance with Know-Your-Customer (KYC) rules. The study estimated that by 2025, AI-based systems will result in cost savings of $460 million for onboarding alone.

Harnessing Digital Solutions: Putting the Needle Back in the AML Haystack
Perhaps the most challenging bank compliance area—and the most obvious use case for a digital-native overhaul—is the Bank Secrecy Act (BSA). Efforts to find money laundering in banking transactions are sometimes likened to a “haystack without a needle.” The industry and regulators are awash in a limitless supply of transaction data. The challenge is to assemble, monitor and analyze it to detect “suspicious” activity that must be reported to FinCEN. BSA officers complain that the AML reporting regime results in a heavy burden for banks without finding much money-laundering. According to some estimates, including by the United Nations, AML efforts worldwide stop less than one percent of financial crime.

One longstanding frustration is that AML systems have traditionally been designed more to comply with federal reporting requirements rather than to find actual crimes. Indeed, banks’ internal alerts for flagging suspicious transactions have a shockingly high false-positive rate of 90 percent. In financial services, one can imagine criminals using AI to invent identities, fake loan documentation, and use increasingly creative means to trick unwitting bank officers or consumers.
Digital innovation holds the potential to make AML monitoring more precise and effective in two key areas.

First, law enforcement and regulatory agencies have taken steps to conduct more useful data analysis of the reports they receive from the industry. This starts with better integration between the Financial Crimes Enforcement Network (FinCEN) and the bank regulatory agencies. Additionally, last year, the Treasury Department released the National Strategy for Combating Terrorist and Other Illicit Financing, which said the government will, among other things, “continue to enhance the use of artificial intelligence (AI) and data analytics in U.S. government efforts to detect and disrupt illicit finance.”

The second positive development is the emergence and growth of regtech firms to better assist banks in almost every area of AML compliance, including KYC rules, automated customer onboarding decisions, sanctions screening, beneficial-ownership requirements, digital identity verification, transaction monitoring, pattern analysis and AML case management. Some regtech firms aim to drastically improve the transaction monitoring process with AI tools such as Machine Learning (ML) and Natural Language Processing (NLP) to identify subtle signs of crime and reduce both false positives and false negatives.

Meanwhile, by 2030, financial institutions can expect significant innovation in the ability of AML data to be shared across firms and between governments. “Privacy-Enhancing Technologies,” or PETs, allow multiple parties to exchange information about potential threats while still preserving customer privacy. Last year, the U.S. and U.K. governments announced a collaboration on prize challenges to encourage innovators to develop PETs. And in June 2023, the Innovation Hub of the Bank for International Settlements shared results of its Project Aurora, finding highly promising results from use of multiple PETs on cross-border data. The potential for safe, widespread sharing of data is opening up the prospect that industry and government can turn the tide against rising levels of global criminal networks that today launder funds through the banking system to reap profits from crimes like trafficking in weapons, drugs, endangered wildlife and human beings.

Credit Access Without Sacrificing Quality

Over the next decade, a digital-native approach to compliance will also make it more likely that lenders will be able to expand the credit pie without resulting in higher loan losses and with less risk of being targeted by enforcement actions. Much as data management tools improve customer onboarding and digital identification verification in the AML area, a growing number of regtech providers are developing digital processes to better flag potential consumer protection issues such as fair-lending violations.

Compliance risk, especially the specific threat of committing unintended discrimination under the “disparate impact” doctrine, has discouraged many financial firms from designing a lending program that is truly inclusive. Lenders worry that when they serve markets where the credit decision is a close call, they may generate patterns of outcomes that can trigger examiner scrutiny, in a space where regulatory standards are largely subjective. However, new technology providers offer hope that lenders can use digital means to expand credit access without added compliance (or credit) risk. Some companies utilize AI to try to eliminate lending bias from an automated underwriting process. Other software providers have developed machine learning (ML) models in credit underwriting to screen for cases of disparate impact, as well as disparate treatment.

A key to this progress is the rising ability to use alternative data to evaluate the creditworthiness of consumers with thin or no credit files. Especially after the 2008 mortgage debacle, lenders are cautious about using consumer data in the underwriting process that is not clear-cut indicators of creditworthiness. But several technology tools show promise in helping lenders determine which newer types of data are accurate predictors of a loan’s performance, while at the same time avoiding patterns that might involve bias. New kinds of data are driving the AI tools noted above, and are also helping enable non-AI approaches.

The most promising example of the latter, so far, is analysis of an applicant’s cash flows, which can help lenders evaluate creditworthiness with less
focus on credit histories. Some startup credit card lenders have already incorporated cash-flow analysis into their underwriting.

One likely result of emerging technology will be a convergence of business and compliance processes and a positive alignment of their goals. In fair lending, it seems likely that new high-tech underwriting tools will enable many banks to “grow in place,” expanding lending inside their current geographic footprints by growing vertically, able to serve more people in their communities with sound and affordable lending.

**Embracing Compliance Tech: A Regulatory Shift towards Digital Innovation**

Utilizing AI, new data and other digital tools increasingly yields better compliance outcomes. However, banks in the future may not have a choice about whether to incorporate them into their compliance process. Their regulators may require it.

A more formal regime mandating improvements in compliance tech would come as regulators around the globe are generally embracing digital innovation as offering practical solutions for both the public and private sectors.

Among regulators worldwide, a global leader in spearheading innovation initiatives has been the U.K.-based Financial Conduct Authority (FCA).

In 2019, Nick Cook, then the FCA’s innovation director, said the agency was seeking to “stimulate innovation within the market that we believe will deliver public value.” (Cook is now the Chief Innovation Officer for the Alliance for Regulation Innovation, or AIR.) He articulated the FCAs interest in seeing AML innovation, and in particular PETs, as well as more investment in digital regulatory reporting.

“These are early examples of our changing approach and they will not be the only occasions or areas where we call out specific issues and problems to which we would like to see further innovation and progress,” Cook said.

Meanwhile, in the U.S., the Department of Justice has updated guidance about corporate compliance programs, which suggests that data analytics are a key factor in the success of such programs.

Among the questions that prosecutors will consider when evaluating a corporate compliance program, the guidance says, is: “Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls, and transactions? [and] Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?”

The same new technologies that are driving regtech can and will be adopted by the regulators, themselves, for suptech. As these kinds of tools prove their ability to find more noncompliance, find it sooner and (once it is installed) lower operating costs, agency use will ramp up. In the U.K. the FCA recently completed its transition to cloud computing and built a shared suptech platform with the Bank of England. Other regulators are
One benefit of adopting regulatory technology (regtech) in banks’ compliance programs—mirrored by adoption of supervisory technology (suptech) at the agencies—will be lower operating costs.

making similar conversions. Many are also working on new systems for “digital regulatory reporting” (DRR) that will give them access to full data, in real time, whenever they want to see it. This enables what the FCA calls a “single view of the firm” that functions as a real-time risk dashboard for each entity and for subsets of the systems.

Consider this: the day is approaching when banks with older, lower-tech compliance programs will be dealing with regulators who know where the risks and noncompliance are, before the bank does. Every compliance function needs to keep pace with that curve.

Proactive Measures for Compliance: Initial Steps toward a Digital-Native Overhaul

The present and future emphasis on new data, AI tools and other technology, and how they will reshape the regulatory process, may seem daunting to bank compliance managers as they weigh both the risks and opportunities of the digital transformation.

To ease the transition, there are relatively straightforward steps that compliance officers can take now in preparation for a digital-native overhaul. At the outset, four important tasks are:

Get educated: Every compliance officer today needs a working knowledge of digital-age technology. They need familiarity with AI, its branches like Natural Language Processing (NLP) and Machine Learning (ML), and especially the new realm of Generative AI tools like ChatGPT and Large Language Models (LLMs). They need to understand blockchains and distributed ledgers, cryptocurrency and tablecoins, developments in central bank digital currencies (CBDCs), tokenization, Decentralized Autonomous Organizations (DAOs), privacy-enhancing technologies, trends in encryption, quantum computing, decentralized finance (defi) and Web3, the metaverse, emerging risks relating to data security, and much more.

They also need to learn new skills relating to change management as technology trends accelerate. They need to understand the concepts of agile workflow, design thinking, and human centered design. Even if the bank has no plans to engage in cutting-edge services, compliance personnel need to deal with the facts that these technologies are converging and reshaping traditional finance, and are doing so at unprecedented speed. The majority of banks are expected to be influenced by these technology trends.

Regulatory agencies, trade associations, technology groups and other organizations offer educational curricula for a variety of business managers on key technology concepts. The American Bankers Association has highlighted technology training platforms on cybersecurity awareness, risk management and more.23 The industry’s growing awareness of digital trends mirrors steps that several regulatory agencies have recently taken to educate personnel.

The FCA holds an annual event known as “Data Week” for its employees. AIR is currently in the process of designing technology education modules to be offered to U.S. regulators.

It’s noteworthy that technology change will almost inevitably outpace legislative and regulatory change. This means that banks will put themselves at risk if they rely on “rules-based” technical compliance strategies to satisfy their regulators. Business innovation will develop in regulatory gray areas, and banks will need to adopt proactive “principles-based” approaches that anticipate future rules and/or withstand scrutiny from subjective regulatory tools like the ban on Unfair, Deceptive, or Abusive Acts or Practices (UDAAP). Doing this well will require CCOs to understand the technology involved.

Ensure the C-suite and Board are involved: Following the financial crisis, many banks elevated the roles of risk managers to include them on the senior executive team, reporting directly to the CEO or COO. In many cases, banks also elevated their Chief Compliance Officer. This leadership framework allows for clear and frank communication between a bank’s most senior managers to:

1. Evaluate the status of a bank’s technology stack;
2. Assess the extent to which an institution is using technology and data to benefit the compliance process; and
3. Consider which types of technology investments should be part of the compliance program over the long term.

If there is not already alignment and information-sharing between the CCO and Chief Technology Officer, that integration should occur sooner rather than later.

Collaboratively innovate with your core provider: As compliance and other regulatory frameworks accelerate on the path to a digital-native future, banks will need to be able to respond to technology developments with agility. Smaller community-based financial institutions are typically reliant on a third-party core processor for maintaining and making changes to their technology platforms. It is vital that those banks have a discussion now with their core provider about what technological innovations will be offered for their banking systems and when these will be available. Armed with this knowledge, the bank can then make direct requests for specific service offerings to improve compliance effectiveness.

As banks increasingly work with regtech vendors other than their core processor, they should seek clarity from their core provider about the level of flexibility in their vendor contract to partner with other providers. Many banks are in the process of establishing the ability to use application programming interfaces (APIs) to make their core functions interact with other vendors and suppliers. Others are evaluating services offered by a new generation of cores, as well as “middleware” providers that can enable easy interfacing.

Banks should also assess and ensure that their vendor contracts of all kinds give them ready access to their own data, without restrictions, delays, or additional fees. Data is the life’s blood of the future of banking, including the future of compliance.

Secure a seat at the digital transformation table: Above and beyond working with changes to the core, compliance leaders need to be in “the room where it happens” as their banks undertake digitization and innovation strategies. Most small banks will increasingly engage with fintechs as third-party vendors and partners to provide the technology that today’s customers demand.
Regtech tools powered by AI and faster processing speeds can help institutions automate the monitoring of anti-money-laundering threats, pore through massive amounts of data identifying fair-lending risk and use alternative credit data in their underwriting systems, among other purposes.

We may be on the verge of a new renaissance of technology innovation that will improve the efficiency and effectiveness of back-office operations that up to now have been limited by analog systems. Imagine a compliance system that actually helps catch the bad guys, expands financial services access and saves money. Compliance managers’ path forward in the digital environment carries definitive risks. However, the sudden emergence of generative AI, the limitless supply of data available to regulators and the financial services industry, and an increasing field of startup regtech providers offering an expanding suite of services, are also reasons to be optimistic about the benefits of a digital-native compliance process.

ENDNOTES
3. apnews.com/article/pentagon-explosion-misinformation-stock-market-96f534790872ded7012e811b5edf47
16. thepaypers.com/expert-opinion/a-new-high-tech-era-for-AML-compliance-in-the-us--1257774
25. www aba.com/training/events/online/technology

ABOUT THE AUTHOR
JO ANN BAREFOOT is CEO and Cofounder of AIR, the Alliance for Innovative Regulation, a nonprofit dedicated to digitizing the financial regulatory system to advance fair finance, to foster an innovative and resilient financial sector, and to combat financial crimes like human trafficking. A former Deputy Comptroller of the Currency and staff member of the U.S. Senate Banking Committee, Jo Ann is a Senior Fellow Emerita at the Harvard Kennedy School Center for Business and Government. She hosts the global podcast Barefoot Innovation and authored the seminal paper, A Regtech Manifesto. Jo Ann advises numerous regulatory bodies and speaks annually to thousands of people throughout the world. In 2020 she was inducted into the Fintech Hall of Fame by CB Insights. Reach her at linkedin.com/in/jbarefoot/