CORPORATE COUNSEL
An ALM Website
corpcounsel.com | July 12, 2019

Disruptive Technology Part 2: Where's the Risk?

By Amanda Groves

This article is the second in a three-part series exploring executives' perspectives on disruptive technologies in the financial services industry. The first installment looked at how the industry is using these technologies.

Credit: Lightspring/Shutterstock.com

The financial services industry is embracing disruptive technology, but executives are also aware of the potential risks it can bring, according to a study conducted by ALM's *Corporate Counsel* on behalf of Winston & Strawn.

The survey found that the level of perceived legal risk depends on the specific technology in question. AI is the area of greatest concern, with 51% of companies seeing it as a significant source of risk. Slightly fewer (50%) cited social banking and P2P lending, which bring the potential for shifting business models, while 42% cited blockchain, where there is still a lot to learn. "With distributed ledger and blockchain, there is a lot of promise and investment, but few successful use cases," says Michael Loesch, co-chair of Winston's Disruptive Technology Task Force. On the other end of the spectrum, only 34% see significant risk in facial recognition and biosecurity technologies, and 18% see no risk at all in that area.

Concerns about AI risk may stem from the fact that AI is a high-profile technology but one that still holds a number of unknowns—which may be troubling for companies that see it having an increasingly significant role throughout the business. In particular, bias in AI-enabled loan underwriting was cited by 45% of respondents as a risk—presumably because financial services companies are aware of studies that have shown that bias can creep into AI loan underwriting, highlighting the potential for unintended consequences with a powerful technology. They also know that it can be difficult to explain how AI systems—which are often opaque, "black box" technologies—produce their recommendations, which is likely to gain the attention of regulators.

Meanwhile, it is not always clear how evolving regulatory frameworks will affect the use of AI. For example, with AI-enabled personal assistants for customers, "banks are still asking what the restrictions are going to be on what the personal assistant can do," says Winston litigation partner Danielle Williams. "Are they just able to read and relay account information? Will they execute transactions? There could be regulatory issues with every aspect of that." AI used in internal processes, such as robotic process automation, could also increase legal risk if the way it is programmed introduces errors into back-office work.

"The ways in which AI is being deployed in the financial space, however, is of lower risk than in other industries where we are trusting AI to make potentially life-altering or threatening decisions," remarked Kathi Vidal, Winston's Silicon Valley managing partner and a former AI developer. "In the financial space, AI not only has the potential to replicate human decision making but also to improve it. In fraud detection, credit analysis, and other applications, we can train neural networks and other AI systems to better, and more blindly, analyze big data to render more accurate but also more equitable predictions," concluded Vidal.

In time, more familiarity with disruptive technologies may actually increase awareness of potential risks. "Some institutions just aren't using disruptive technologies to their fullest capacities yet," says Basil Godellas, head of Winston's Financial Services Regulatory Practice. "For example, respondents had fairly low concern about facial recognition, biometrics, and biosecurity solutions. But most institutions are just dipping their toes in the water with these technologies—and I think their concerns about risk may grow as they have more exposure to them." Evolving legal frameworks may also increase those concerns. The 2008 Illinois Biometric Information Protection Act, for example, regulates how companies collect biometric information, such as fingerprints and retinal scans. More recently, a number of other states have passed or proposed similar biometric data privacy laws.

Beyond any specific technology, financial services companies clearly see risk in the cybersecurity and data privacy realm. (As mentioned above, respondents cited this as a top barrier to implementing disruptive technology.) The industry has long experience with the challenges of keeping sensitive data safe, as well as with the legal and regulatory costs of failing to do so. But disruptive technologies raise the security bar significantly because they rely on large amounts of quality data—often sensitive data about customers—to operate, provide services, and create insights. And that data has to be managed, protected, and shared safely with a growing number of applications.

At the same time, regulations around data privacy and cybersecurity are evolving. Take, for example, the EU's General Data Protection Regulation, which went into effect last year and significantly strengthened privacy regulations—and penalties for noncompliance. Or consider the California Consumer Privacy Act of 2018, slated to go into effect in 2020, which has some of the most stringent privacy mandates in the United States. Such regulations, coupled with the advent of disruptive technologies, only make compliance more complex.

Regulators: Looking at Disruptive Technology

Executives worry about fintech and disruptive technologies bringing unwanted attention from a variety of legal and regulatory sources—indeed, 41% of respondents point to investigations and civil enforcement actions by federal agencies as the largest technology-related legal/regulatory threat. Many worry about actions by industry groups (32%), state regulators (28%), DOJ and state attorneys general (26%), and private civil plaintiffs (24%).

Meanwhile, nearly half say they are concerned with technology-related antitrust issues and the possibility of antitrust enforcement—driven in part by a sense that the rules are lagging behind advancing technology. "In financial services, there is an overarching concern that the antitrust laws as they are drafted today might not be sophisticated enough or flexible enough to deal with new disruptive technologies," says Susannah Torpey, a partner at Winston & Strawn.

There are other antitrust implications to consider as well. In a technology-driven world, collaboration and working in partner ecosystems are both easier and more important. When setting up blockchain consortia or working with others in the industry to set technology standards, "you have to be very careful that this increase in coordination is well managed, so that you don't find yourself exchanging information with your competitors that leads to anti-competitive effects in the market place," commented Torpey.

Disruptive technologies essentially increase the importance of data in business, and AI specifically makes it easier to gather and use data from a wide variety of internal and external sources. Thus, these new technologies may increase the risk that regulators will consider data a source of market power when assessing mergers and acquisitions. And because disruptive technologies can drive innovations that quickly alter competitive dynamics, companies that succeed with new approaches may find themselves under increased scrutiny. "A startup financial services company that does something new might quickly gain dominant share of a niche market, which could put them at a much higher risk of an antitrust violation," says Torpey.

In general, fintech and disruptive technology are moving quickly, and regulators sometimes struggle to keep up—which itself presents challenges to financial services companies trying to balance innovation and compliance. But regulators are paying close attention to these technologies. The U.S. Commodity Futures Trading Commission, for example, has established a LabTechCFTC program designed to keep the commission in close touch with technology innovators—and other agencies have set up similar programs. Perhaps with an eye toward those efforts, nearly seven out of 10 financial services companies believe that regulators are keeping up with the use of disruptive technologies in the industry. But in reality, that can be a challenge. "Regulators are doing positive things like LabTech to keep up with technology, but they are often still playing catch-up," says Loesch. "They have to use the tools and laws that they have, and sometimes those are not fit for purposes in the disruptive technology space. There are tensions because the normal regulatory framework doesn't always fit precisely with how the new technology operates. And that can lead to costly investigations and even enforcement actions."

The next installment in this series examines strategies for managing technology-driven risk.

Amanda Groves *is co-chair of Winston's Complex Commercial Litigation Practice. She has successfully represented consumer product companies, national retailers, and lending institutions in consumer protection cases since 1996.*

Reprinted with permission from the July 12, 2019 edition of CORPORATE COUNSEL © 2019 ALM Media Properties, LLC. This article appears online only. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 016-07-19-03