Debevoise & Plimpton

October 2018

TMT INSIGHTS
From the Debevoise Technology, Media & Telecommunications Practice

Key Insights from the New York AI in Finance Summit

The fast developing fields of artificial intelligence ("AI") and machine learning are bringing new opportunities—and new regulatory and compliance concerns—to the FinTech and financial services sectors. At the recent AI in Finance Summit held in New York, industry leaders outlined the key developments they are seeing:

- ***Regulators are embracing AI and machine learning.*** Regulatory bodies such as the Securities and Exchange Commission and the Financial Industry Regulatory Authority ("FINRA") are harnessing machine learning to carry out their supervisory functions (often referred to as "SupTech"). For example, FINRA is using algorithms to detect potential market anomalies or misconduct occurring at broker-dealers, including by identifying suspicious word clusters in termination notices for registered representatives. Once found, FINRA can further investigate and alert companies and regulators of these schemes.

  As regulators continue to enhance their own machine learning capabilities, they are also providing detailed guidance for the industry. FINRA's recent report, *Technology Based Innovations for Regulatory Compliance ("RegTech") in the Securities Industry*, for example, outlines procedures and control systems that regulated firms should consider implementing for their machine learning initiatives, including:

  - Developing data governance programs to ensure the accuracy and quality of the underlying data
  - Implementing procedures to identify and mitigate material errors or malfunctioning
  - Training non-technical staff on the functions and limitations of the tool
  - Updating supervisory procedures to address any machine learning capabilities that have been outsourced to third parties
  - Designing procedures to protect customer records and data
  - Providing accurate notices about the company's data sharing policies

- ***New technologies promote data sharing while protecting privacy and security.*** Machine learning is driven by data, and many companies are increasingly interested in linking or sharing data across businesses or jurisdictions. Combining these datasets may not only create privacy risks—think of the 2017 Equifax data breach—but it also may run contrary to data protection laws, such as the EU General Data Protection Regulation.

The traditional trade-offs between AI and privacy may be shifting, however, as technological solutions develop to enhance privacy protections. For example, a process called "fully homomorphic encryption" allows companies to process large, sensitive datasets—even those stored remotely or on the cloud—without ever needing to decrypt and expose the underlying data. This approach may enable companies to share or leverage this encrypted data for machine learning, while potentially also complying with applicable data-protection regimes.

- ***Malicious actors are likely to target AI.*** The scope and value of machine learning platforms makes them tempting targets. New threats must be continuously anticipated and prevented. Researchers have recently shown that "adversarial example attacks" can fool machine learning models into generating incorrect conclusions—for example, image recognition algorithms can be manipulated into mistaking "STOP" signs for "Yield" signs, and photos of rifles can be misidentified as helicopters. In the financial services industry, an adversarial example attack could be used to disrupt fraud detection algorithms or inappropriately trigger stock sales. Furthermore, once an attack vector is successful against one machine-learning model, it can often be deployed on others.

  Staying ahead of evolving threats begins with knowing the answers to two key questions: first, who stands to gain from attacking your machine learning models; and second, how susceptible are your models to a potential attack? Defenses to adversarial attacks are being developed to protect machine learning systems, and while this work is still in its early stages, it will be an important space for companies to monitor.

- ***Regulatory sandboxes are becoming tools for collaboration and innovation.*** The financial services industry has been one of the earliest adopters of AI and machine learning. As such, it is uniquely positioned to engage with regulators about how to develop standards for AI, while simultaneously encouraging innovation.

  One proposed solution has been the creation of "regulatory sandboxes"—programs that allow companies to test new products or services for a limited time under modified regulatory requirements. Regulatory sandboxes may provide a mechanism for companies to innovate on new technologies at lower cost, and without fear of compliance penalties. For regulators, sandboxes also offer opportunities to stay engaged and educated about the latest technological developments. Meanwhile, innovators can work with regulators to ensure that their technologies align with existing regulations.

  As we have previously noted, the U.S. Treasury Department and Consumer Financial Protection Bureau ("CFPB") have recently called for the use of regulatory sandboxes for certain FinTech companies (See Debevoise Update, *A Turning Point for FinTech? OCC and Treasury Signal Commitment to Financial Innovation*), while this year Arizona became the first state to launch such a sandbox, a two-year project under the oversight of the state's Attorney General's Office (See Press Release, *Arizona Becomes First State in U.S. to Offer Fintech Regulatory Sandbox*). Regulatory sandboxes have also been adopted in other jurisdictions, such as the United Kingdom, Canada and Hong Kong (See Debevoise In Depth, *Thinking Inside the Box: The UK FCA Sandbox, a Playground for Innovation*).

On August 7, 2018, the U.K. Financial Conduct Authority, CFPB Office of Innovation and ten other regulators announced the creation of a Global Financial Innovation Network ("GFIN") (See Consumer Financial Protection Bureau, *BCFP Collaborates With Regulators Around the World to Create Global Financial Innovation Network* and *Global Financial Innovation Network (GFIN), Consultation Document*). GFIN is currently exploring the creation of a "global sandbox," which would provide a global platform for companies to engage in cross-jurisdictional testing of emerging technologies, such as AI, in consultation with multiple regulators. GFIN has solicited comments from companies and regulators on this proposal, and further developments will likely be announced in the near future.

Contributors

Anna R. Gressel
Associate – New York
argressel@debevoise.com
T+1 212 909 6485

Michael A. Diz
Partner – New York
madiz@debevoise.com
+1 212 909 6926

Jonathan E. Levitsky
Partner – New York
jelevitsky@debevoise.com
+1 212 909 6423

Jim Pastore
Partner – New York
jjpastore@debevoise.com
+1 212 909 6793

Michael Schaper
Partner – New York
mschaper@debevoise.com
+1 212 909 6737

David G. Sewell
Counsel – New York
dsewell@debevoise.com
+1 212 909 6755

About Our Practice

Debevoise's far-reaching TMT practice is a top choice for clients seeking trusted advisors for complex deals or high-stakes cases. Highly ranked in a variety of categories in the technology, media and telecommunications space, Debevoise has what *Chambers Global* describes as a TMT practice that is "full-service and creative, and has a global presence." For more information please visit our Technology, Media and Telecommunications practice page.