Guidepost

OUT OF MANY, ONE? — THE FUTURE OF U.S. FINTECH REGULATION

As published in FinTechWeekly August 29, 2018.

Not for the first time, the federal government and states are at odds over the future regulation of FinTech.

On July 31, 2018, the Office of the Comptroller of Currency (OCC) at the U.S. Department of the Treasury (DoT) announced it would begin accepting applications from FinTechs for special bank charters, which would allow them to operate nationally. But individual states and inter-state organizations are strongly opposed. The Conference of State Bank Supervisors (CSBS), which brought an unsuccessful lawsuit against the OCC last year to stop the charter being introduced, has declared that it is 'a regulatory train wreck in the making.'

The irony is that both sides of the debate want greater consistency. The key difference is determining who should drive the change. As this battle continues, how can U.S. FinTechs approach this complex regulatory landscape, protect themselves and their customers from financial crime, and change potential risks into competitive advantages?

No Single Framework

Part of the difficulties FinTechs face while navigating the U.S. regulatory environment are not only the different layers of government—state and federal—but also the lack of one single type of FinTech. Digital payments firms, for instance, are seen as money service bureaus (MSBs) under the federal Banking Security Act (BSA) and have to register both with the Financial Crime Enforcement Network (FinCEN) at the DoT, as well as gain a state license. Cryptocurrency exchanges are also considered MSBs, because they transmit funds, but initial coin offerings (ICOs), where a new cryptocurrency is offered in return for investment in the startup, is considered a form of security and is subject to the Securities Act and Securities Exchange Act, regulated by the Securities and Exchange Commission (SEC). The table below provides a simplified view of financial crime risks, regulations, and the FinTech sectors that might be affected.

What Do Both Sides Want?

First, the states are keen to see licensing for FinTechs remain in their hands, and there have been collective moves to increase alignment and streamlining across the states for all forms of non-bank financial activity. CSBS's 'Vision 2020' reinforces this with what it calls is "a series of initiatives…to modernize state regulation of non-banks, including financial technology firms." The program aims to ensure that by 2020, there will be an integrated state licensing and supervisory system across all 50 states. This includes the redesign of Nationwide Multistate Licensing System (NMLS), the core technology platform used by state bank regulators, the introduction of a Fintech Industry Advisory Panel, harmonization of state supervision, and education programs to improve bank and non-bank interaction.

According to the recent DoT report, 'Nonbank Financials, Fintech, and Innovation,' the federal government wishes to see financial innovation continue, but within a more consistent regulatory framework. The report suggests a range of possibilities, such as state alignment through 'model laws', license harmonization, FinTech/Financial Service provider partnerships, as well as the OCC 'special bank' charter. Indeed, the OCC itself has said that the special charter is only one option, and it is conceivable that a hybrid approach might develop over time, through negotiation between the states and the federal government. All sides seem to want to get to the same destination, but have varying views about who should be in charge.

What does this mean for Financial Crime Risk?

From the perspective of identifying, managing and mitigating financial crime risks in the U.S. FinTech sector, there are plenty of positives in these developments. Variations in types of regulation between jurisdictions can create vulnerabilities in a system that can abet money launderers. Federal legislation apart, if one state has significantly less demanding requirements for company licensing than another, then it could become a portal through which criminal funds are most easily 'placed' in the financial system—stage one of the money laundering cycle. And from there, the funds can be 'layered'—sent through multiple accounts in the financial system (stage two)—before being 'integrated' into a seemingly legitimate account (stage three), quite possibly in a state with higher licensing requirements. If there is greater and more demanding standardization, and more consistent application of the standards, this should then help to reduce financial crime risk overall.

How should FinTechs respond?

However, it is important that FinTechs do not interpret this positive trend in the wrong way. Improved and consistent regulation can reduce some of the niches in which financial criminals can operate. However, it does not eliminate financial crime risk, because, as experience has shown, those who launder criminal funds, evade sanctions and tax, and finance terrorism, are amongst the most creative people in the world.

So rather than becoming caught up a traditional compliance 'tick box' culture, or following regulatory battles, FinTechs should focus first on the actual financial crime risks themselves. Regardless of the final outcome of the tug of war

between the states and the federal government, FinTechs must consider how to manage their risks in this area, in the best interests of themselves and their clients. This isn't just good for risk management and compliance—it is also good for business.

FinTech firms should consider a simple four step approach:

1. **Undertake a financial crime risk assessment.** This is essential to knowing your key vulnerabilities and then being able to measure your efforts to reduce them over time. This requires challenging assumptions, testing vulnerabilities, and working in detail to understand the precise extent and nature of money laundering and other risks to which it could be exposed.
2. **Understand financial crime typologies.** Make use of available typologies studies related to certain offenses, to understand potential exposure and assess whether any unknown risks do in fact exist. Given the anonymous character of many transactions on online platforms, FinTechs should pay special attention to the risks from different types of fraud, such as synthetic identity fraud.
3. **Tailored systems.** Seek to build systems and processes that are specifically designed for the risks FinTechs are likely to face. For example, although all financial institutions are subject to U.S. sanctions laws, providers involved in cross-border transactions should give higher priority to screening for potential evasion. A risk focused approach is more likely to create a healthy and proactive compliance culture.
4. **Create indicators and use data:** FinTechs should leverage the skill they have in utilizing data to decipher indicators of specific money laundering risks. They should continue using these indicators and supporting data as key performance indicators on a regular and scheduled basis. This is invaluable for managing risk and makes the process of future conversations with auditors and regulators considerably easier.

Understanding and implementing this process is key to stopping financial crime in its tracks and helping transform risks into opportunities.

****CO-WRITTEN BY GEMMA ROGERS, CO-FOUNDER, FINTRAIL LTD

Gemma Rogers is the co-founder of FINTRAIL LTD., a financial technology compliance consulting firm. She has a passion for changing the terms of debate around financial crime risk management, debunking the lethargic tick-box concepts of old and focusing on intelligent, inclusive and business-focused solutions. Drawing on her wealth of experience across disruptive services, international banking and the public sector, Gemma brings clients deep domain knowledge of financial crime risks, as well as an ability to execute intelligent frameworks across both emerging platforms and established financial services.

JULIE MYERS WOOD

Chief Executive Officer

As the Chief Executive Officer of Guidepost Solutions, I focus on helping corporations resolve problems with government agencies, and ensure they are proactively addressing compliance requirements. Prior to joining the private sector, I held leadership positions with the U.S. Departments of Homeland Security, Commerce, Treasury and Justice. This includes serving as the Head of Immigration and Customs Enforcement, Homeland Security's largest investigative component, as well as the Assistant Secretary for Export Enforcement and the Chief of Staff for the Criminal Division at the Department of Justice. Throughout my government and private sector career, I have helped develop, implement and execute compliance programs and crisis management plans and responses across a wide range of industries for numerous companies. I am nationally recognized as a speaker for my expertise on compliance, security, immigration and other law enforcement issues and have testified before Congress.