Michael Held: The first line of defense and financial crime

Keynote address by Mr Michael Held, Executive Vice President of the Legal Group of the Federal Reserve Bank of New York, at the 1LoD Summit, New York City, 2 April 2019.

* * *

As prepared for delivery

Good morning. It's an honor to join you at the 1LoD Summit. As always, the views I express today are my own, not necessarily those of the Federal Reserve Bank of New York or the Federal Reserve System.[1]

Introduction

I'm very grateful for the return invitation. I have to be honest with you, though. When Paul approached me to speak again this year, I was wary. What would you all think of having to listen to me again? The phrase "cruel and unusual punishment" came to mind. Then I was reminded of an old joke. To paraphrase W.C. Fields: First prize, one Held speech. Second prize, two Held speeches. That's a much more pleasant way to think of a return engagement. So congratulations on second prize.

I really do appreciate this opportunity for two reasons. *First*, I want to express again my support for risk managers in the first line of defense. Supervisors and the industry are often on opposite sides of the table—or opposite sides of the "v.," as they say in my line of work. But, in many instances, our goals are shared. "Safety and soundness"—the guiding principle of microprudential supervision—is a shared objective, even if supervisors and the industry sometimes disagree how the concept applies to particular facts. I think we can agree that your work as first-line risk managers promotes safe and sound operations within your organizations. So let me begin with my thanks for your continuing efforts.

Second, there are some things that I would like to get off of my chest. My topic this morning is financial crime—more specifically, crime that converts and corrupts the payment system to achieve its ends. This includes theft, fraud, money laundering, sanctions evasion, bribery, kleptocracy, cyber-terrorism, and electronic sabotage. Combatting financial crime should *not* be an issue that finds supervisors and industry on opposite sides of the "v." It is in everyone's interest—supervisors and their public constituents; the industry and its customers—to keep crime and the proceeds of crime out of the payment system. Of course, no one is perfect. But we must be honest with each other about what we're doing, what we're *not* doing, and how we can improve.

Let me highlight just one example to demonstrate why I am so focused on financial crime right now. As I'm sure many of you have read, in February 2016 international criminals used fraudulent wire transfer instructions to steal and launder many millions of dollars from Bangladesh Bank's account at the New York Fed. Bangladesh Bank is the central bank of Bangladesh. Some of those funds have been recovered, but Bangladesh Bank is still working to recover most of its loss. We at the New York Fed are still helping them to do so. Simply put, it was not just Bangladesh Bank that was wronged. The New York Fed—my client and employer of more than 20 years—was wronged as well. So I come to you today not as a dispassionate observer. I come to you today bearing the scrapes and bruises and scars of our own experience at the New York Fed.

This morning, I will speak about where we are and where I think we should go from here. My message, in brief, is that we are all in this together. The integrity of the payment system is critical to the U.S. and global economy. Financial institutions and the official sector must do their utmost to protect the system from financial crime.

Where Are We Now?

The payment system can be used to facilitate many types of crime. Fraud and theft have accompanied money transfers for as long as there has been money. The Romans considered counterfeiting to be a form of *falsum*, which was a fraud against the public.[2] And, of course, Willie Sutton provided the timeless, common-sense explanation for bank robbery.

Money laundering is, by contrast, a more recent development in criminal law. In the United States, anti-money laundering law reflects an evolution in focus from banknote tracking to combatting narco-trafficking to counterterrorism. Rather than take you through the legislative history of this evolution, I want to refer you to the Financial Crimes Enforcement Network—or "FinCEN," for short. Its website contains short and accessible histories of major anti-money laundering laws.[3] These summaries highlight the important public goals of the Bank Secrecy Act and other anti-money laundering statutes—why they are more than just a compliance cost. One theme that emerges is the increasing reliance on banks and other financial institutions to safeguard the payment system. Our laws and regulations increasingly bring the industry into partnership with the government on combatting national security risks to the United States and financial crime.

Anti-money laundering is not just a matter of historical record. Our rules continue to evolve. For example, in 2016 the Treasury Department updated its regulations to require that banks and other financial institutions verify the identity of the natural persons—that is, the "beneficial owners"—who own or control companies that hold accounts.[4] The beneficial owner rule, like other "know your customer" rules, is a regulatory floor, not a ceiling. Covered firms can take the initiative to implement more stringent internal rules based on their risk. Indeed, in December 2018, the federal banking agencies published guidance that encouraged innovation in anti-money laundering compliance—pilot programs that exceed the legal minima, or at least make compliance more efficient.[5]

Experiments in ratcheting up internal thresholds are welcome. As I have said in other contexts, one challenge in a rules-based regime is that the pace of rulemaking is not always commensurate with the pace of rule breaking.[6] Complying with minimum legal thresholds may not be sufficient in all circumstances to appropriately mitigate risk to your firm or the payment system.[7] Technology has greatly expanded access to the payment system. Many of us—everyday consumers, that is—effect payments not only directly through our banks, but also through various "fintech" intermediaries. There is much good in this, but technology is not risk-free. The creative development and application of technology can create opportunities to improve the payment system. Technology also creates new opportunities to compromise that system.

Take, for example, the nascent challenge presented by the development of digital currencies. The New York State Attorney General's office estimates that more than 1,800 virtual currencies are exchanged around the world.[8] Many digital currencies use distributed ledger technologies, which can help institutions achieve efficiencies in customer due diligence programs. Distributed ledgers also promote traceability, which in theory assists law enforcement. That said, the use of private exchanges for these digital currencies may facilitate anonymity, which tends to help the bad guys.

My concerns, however, are less about the technological frontier, and more about well-established risks to the payment system. Recent press reports about financial crimes involving 1MDB, Danske Bank, Swedbank, and, yes, Bangladesh Bank make no mention of fancy new digital currencies. Rather, if press reports are to be believed, these cases are to varying degrees about theft, fraud, greed, and corruption.

Less covered in the press is trade-based money laundering—that is, using legitimate trade to

hide illicit sources of funds. The United States is particularly vulnerable to trade-based money laundering because more than half of the world's trade is denominated in U.S. dollars.[9] The Department of Homeland Security and the Drug Enforcement Administration have warned for years that a large amount of illicit narcotic payments occur through low-tech solutions like over- or under-invoicing of goods, false documentation, or phantom shipping.[10] These methods give illegitimate transfers the appearance of ordinary transactions. FinCEN has warned against the use of "funnel accounts" to facilitate trade-based money laundering of narcotics proceeds, and has provided the industry with a list of red flags associated with such activity.[11] Trade-based money laundering can also be used to evade sanctions regimes, sometimes through money service businesses or general trading companies.[12]

The extent of financial crime from a global perspective is simply staggering. According to the United Nations Office on Drugs and Crime, the amount of money laundered globally in one year could be as much as $2 trillion.[13] That's five percent of global aggregate gross domestic product.

If the scale of global financial crime is too large to contemplate, let's focus instead on segments that are local. A few years ago, the television show 60 Minutes covered an undercover operation that captured on video fifteen out of sixteen Manhattan lawyers offering advice on how an African official could secretly move funds into the country.[14] The investigator posed as an adviser to an African minister of mining who managed to accumulate millions of dollars for personal use—expensive real estate, a jet, and a yacht. In the end, no firms actually took on the client. These were just preliminary meetings. And they were a set-up. No actual crimes were committed. Still, only one lawyer out of sixteen told the undercover investigator to get lost. What an eye-opener. As a lawyer and a central banker—and as a New Yorker— I found this report deeply troubling.

Where Do We Go From Here?

So that's where I see us today. Where do we go from here? Let me share some ideas, which are not mutually exclusive.

Build Good Habits

For starters, let's be honest about "looking the other way." Many financial institutions have, at times, turned a blind eye to evidence of money laundering, sanctions evasion, corruption, kleptocracy, and plain theft. Over time, some institutions become weak links in our system when they take on riskier clients, perhaps in order to chase profit, without developing the ability to manage those relationships in a responsible way. Often these relationships start small: one low-value, ethically suspect transaction. But it leads to another and another to the point where the money is simply too good to turn away, no matter how many red flags there are. There may be less pecuniary explanations too. Regardless of the profit potential, our sensitivity to warning signs can fade from lack of practice. For every time we look the other way, it is incrementally easier to ignore the next instance. On the flip side, each time we intervene, the next intervention is easier too. Effective compliance gets better with practice. Like ethics, it needs to be a habit.

And don't think that the bad guys don't notice a firm's reputation—or, dare I say, its culture. Word spreads quickly. A law firm or accounting firm or auditing firm can quickly become known for being "creative" in its approach to an internal investigation or issuing a tax or audit opinion. The same goes for corporate reputations for strong and weak compliance programs, or high or low tolerances for risk. Clients may be attracted to firms with reputations aligned with their goals, for good or ill. So, my first word of advice on where to go from here is to safeguard your corporate reputations by developing good habits.

Just Because It's Legal, Doesn't Make It Right

That's very high-level, prudential advice—not legal advice. A second point I'd like to emphasize is to avoid cabined views of what's permissible or impermissible. Just because something is legal, doesn't make it right.

I'm a lawyer, and I like to say that legal expertise is what gets you into the room. Knowing the law is necessary for professional legitimacy. But, in my view, it is not sufficient. Lawyers also have to consider the bigger picture—the purpose of relevant laws, the client's needs, common sense, and fairness. Those same inquiries should be on the minds of other professionals—including risk professionals in the first line of defense.

I mentioned earlier the recent "beneficial owner" regulations. Those rules are part of the customer due diligence regime for financial institutions. The rules tell you the information firms are required to gather and retain to help keep financial crime out of the banking and payment systems. They do not, however, directly answer the question, "Is this the type of customer we want to do business with?" That question requires judgment that is not the exclusive domain of lawyers. The answer will depend not on laws and regulations, but on your institution's purpose and principles.

Manage Account Relationships

One area where the difference between what's legal and what's right is immediately relevant is the management of customer account relationships, including accounts for respondent banks. I know that this can be tricky. Banks do not want to take on unnecessary legal and reputational risk for the weaknesses and failures of account holders. Nor do banks want to needlessly disrupt or impair the efficiency and speed of the payment system. But that system is under attack. Perhaps we need to think differently about risks, benefits, and costs.

An especially difficult decision is whether to close accounts for respondent banks with a demonstrable record of mismanaging their risks of money laundering and other financial crime. I suspect that many firms will say that they already do this. But they may not do it enough, frankly. Or at the least, they may not ask enough questions when confronted with serious red flags about a respondent bank's activities. It is a process that requires careful attention. If a particular bank, or other financial services provider, is unwilling, or even truly unable, to do their part to protect the payment system, then perhaps they should not be part of it.

To be crystal clear: I do not support the large-scale, regionally focused reduction of the availability of correspondent banking services, sometimes referred to as "de-risking." The industry has been criticized for "de-risking" with a broad sword. I am recommending a scalpel. My concern is how correspondent banks protect themselves and the payment system from *specific* institutions that have a demonstrated, and unremediated, history of unfairly exposing others to their risks.

Client-facing roles are critical to identifying customers that do not play by the rules. The Federal Financial Institutions Examination Council—or "FFIEC"—publishes examples of red flags in its interagency exam manual.[15] Many of these examples require an understanding of ordinary customer behavior in order to spot unusual behavior. Moreover, reasons for suspicion may not be apparent from transmittal records, and can be outside the lens of automated compliance filters, despite their technological sophistication. What makes one transmittal of funds different from another is *purpose*. An understanding of purpose often comes from meeting a customer in person and speaking with her about her business goals.

Improve Communication

One final way forward is to improve communication and information sharing. Here are some questions you might consider.

Within your firms, how does the front office communicate with the control and audit functions about money laundering risk? Is there a frank discussion about common challenges? Or do those discussions resemble depositions or some other defensive exercise?

Between and among firms, do you take advantage of inter-bank information sharing opportunities pursuant to Section 314(b) of the USA PATRIOT Act? [16] If you are a smaller, community-oriented bank, how are you using recent federal guidance that encourages collaborative arrangements that pool anti-money laundering resources?[17] Regardless of size, does your firm insist that customers use the proper SWIFT message type with all the required fields completed in the right format? And, if your firm processes high-risk activity with limited transparency, do you ask respondent banks to supplement payment messages with additional information?

When communicating with the government, how helpful are your suspicious activity reports—or SARs, for short? Are you filing them in the spirit in which they were intended, or for defensive purposes? Are you picking up the phone to call law enforcement when you file a SAR that presents heightened concerns and perhaps should not wait to run through the formal reporting and referral process? And, in response to a terrorist attack or other significant national security event, is your bank proactively searching its payment activity to see if it has potentially relevant information?

One question that I get asked from time to time is if law enforcement can share more information about the activity reported in SARs. I believe law enforcement is always looking for ways to enhance the effectiveness of its information sharing. I want to recognize FinCEN's efforts to share more information via its public website and in its reports to Congress about the information it collects from the industry through SARs. The New York Fed also tries to do its part. It hosts three major conferences every year in which the FBI, FinCEN, local law enforcement, and financial firms discuss financial crime—especially terrorist financing, money laundering, and cyber-crime. We do our best to act as a liaison between banks and law enforcement officials. We'll keep at it.

Conclusion

Stepping back, I'd encourage you to consider as well what your firm's response to financial crime says about its purpose and culture. What does it say about the role of the financial services industry in society? And, to get personal for a moment, how does that response make you feel about where you work and how you make a living?

From where I sit, gaps in AML and other payment system defenses make a terrible impression because of the terrible things funded through illegal payments. When criminals take advantage of your firms and our financial system to make use of their ill-gotten gains, they make every institution involved play the fool. And here I am going to use the "M" word: morals. Now I know that whenever a lawyer starts talking about morals, eye rolling ensues—often justifiably. But I do think that detecting and deterring financial crime is not just a legal obligation. It is a moral one.

Thanks for letting me get all of that off of my chest. I'm honored that you wanted me back this morning. Forums like this highlight important issues and choices. Make the right choices, not just the legal ones. I wish you all a good conference. Thank you.

---

[1] Richard Charlton, Meghan McCurdy, Brett Phillips, Thomas Noone, Sean O'Malley, and Edward Silva assisted in preparing these remarks.

[2] *See* Adolf Berger, *Encyclopedic Dictionary of Roman Law* 467 (1953). *See also* Marcus Tullius Cicero, *In Verrem* 2.1.108 (tracing the crime of counterfeiting to the Cornelian laws).

[3] FinCEN, History of Anti-Money Laundering Laws.

[4] 31 C.F.R. § 1010.230.

[5] SR 18–10: Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing, Dec. 2, 2018.

[6] *See* Michael Held, Reforming Culture and Conduct in the Financial Services Industry: How Can Lawyers Help?, Remarks at Yale Law School's Chirelstein Colloquium, Mar. 8, 2017.

[7] *Cf.* Preet Bharara, Criminal Accountability and Culture, Remarks at the Federal Reserve Bank of New York's Conference: Reforming Culture and Behavior in the Financial Services Industry: Expanding the Dialogue, Oct. 20, 2016 (criticizing a "culture of minimalism," in which firms "do the least amount possible to be in some kind of compliance with rules").

[8] Virtual Markets Integrity Initiative Report, Sept. 18, 2018.

[9] *2018 National Money Laundering Risk Assessment* 6.

[10] U.S. Immigration and Customs Enforcement, a division of the Department of Homeland Security, created its Trade Transparency Unit in 2004.

[11] FinCEN Advisory: Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML, May 28, 2014.

[12] Office of Foreign Assets Control, Advisory on the Use of Exchange Houses and Trading Companies to Evade U.S. Economic Sanctions Against Iran, Jan. 10, 2013.

[13] United Nations Office on Drugs and Crime, Money Laundering and Globalization.

[14] Debra Cassens Weiss, Group goes undercover at 13 law firms to show how US laws facilitate anonymous investment, *ABA Journal*, Feb. 1, 2016.

[15] Federal Financial Institutions Examination Council, *Bank Secrecy Act Anti-Money Laundering Examination Manual, App'x F ("Money Laundering and Terrorist Financing 'Red Flags'")*.

[16] Section 314(b) of the USA PATRIOT Act is not codified in the United States Code, but is available as a historical note to 31 U.S.C. § 5311. The operative rule appears in Department of Treasury regulations. *See* 31 C.F.R. § 1010.540 ("Voluntary information sharing among financial institutions").

[17] SR 18–8: Interagency Statement on Sharing Bank Secrecy Act Resources, Oct. 2, 2018.