TESTIMONY OF

Kathryn Haun Rodriguez

Former Assistant U.S. Attorney, U.S. Department of Justice
Lecturer, Cybercrime and Financial Technologies, Stanford University
Current Member of the Board of Directors, Coinbase Global, Inc.[1]

BEFORE THE

United States Senate
Committee on the Judiciary

"Modernizing AML Laws To Combat Money Laundering and Terrorist Financing"

PRESENTED at Dirksen Senate Office Building, Room 226
November 28, 2017
10:00 am

[1] The views expressed herein reflect my own personal views and not necessarily those of the institutions with which I am affiliated.

Chairman Grassley, Ranking Member Feinstein, and Members of the Committee, thank you for inviting me to testify on the important topic of modernizing our laws to combat money laundering and terrorist finance.

Until several months ago, I was a federal prosecutor with the U.S. Department of Justice (DOJ), a position I held for over a decade. Most of my time at DOJ was as an Assistant U.S. Attorney in San Francisco, where I also served as the first Digital Currency Coordinator. Previously I held senior roles at DOJ headquarters in the National Security Division and the Attorney General's office and was a prosecutor in the Eastern District of Virginia. I teach a course on financial technologies and cryptocurrency at Stanford University, and recently joined the Board of Directors of Coinbase Global, Inc., where I chair its Audit and Risk Committee. I also advise technology companies and investment funds.

During my time as a DOJ prosecutor, I worked cases ranging from national security to violent crimes to corporate and cybercrimes. I prosecuted RICO murders, organized crime, outlaw motorcycle gangs, armed robbery crews, and prison gangs. But I also prosecuted corrupt government officials, identity thieves, bank executives, and international cybercriminals. Although these perpetrators were very different people, they all had one thing in common: Money.

Money lay at the heart of every one of the criminal enterprises I just mentioned. And really, most criminal activity is motivated by money. Money laundering, of course, is the process of disguising criminal proceeds and integrating them into the legitimate financial system. It simultaneously conceals criminals' ongoing affairs and taints the integrity of the financial system.

The World Bank and IMF estimate that every year between $2.17 and $3.61 trillion U.S. dollars are laundered. Criminals are willing to test out new methods of laundering and are early adopters of new technologies. Because of this our AML laws must also evolve, especially given the increased use of the global financial system by money launderers, terrorist financers, drug traffickers, transnational organized criminals, and cybercriminals to place their financial transactions out of reach.

This morning I would like to address two sections in the proposed bill that I believe would have the greatest effect in the largest number of cases: (1) the ability of U.S. law enforcement to obtain foreign bank records under Section 15; and (2) Section 18's criminalization of the concealment or provision of false information to a financial institution concerning account and asset ownership. Although time constraints prevent me from addressing all twenty sections, I have encountered issues that other sections of the bill address and of course welcome your questions.

SECTION 15

The banking system has become significantly more globalized over the past few decades. And today's criminals make extensive use of this global financial system to channel funds across borders for cybercrime, terrorist financing, drug and human trafficking, public corruption, white collar, tax evasion, and many other crimes. But law enforcement's powers have not kept pace with this globalization, and its ability to investigate the transnational movement of money in furtherance of illicit activities is hampered as more and more records reside with foreign banks.

Section 15 makes clear U.S. law enforcement can obtain foreign banking records when they are investigating a U.S. crime and where the subject bank has a presence in the U.S. Law enforcement's ability to timely gain access to records in such circumstances is critical because following the money is a key piece of evidence in solving nearly any crime and because money can quickly be moved. These bank records contain transactions, of course, but they are much more than that: they show relationships between co-conspirators and they show what legal entities are being used as the vehicles of criminal activity.

In theory, under existing law the government can issue grand jury subpoenas to obtain foreign bank records where the bank has (1) a U.S. branch; or (2) a correspondent account with a U.S. bank. *See, e.g.* 18 U.S.C. Section 5318; *In re Grand Jury Proceedings Bank of Nova Scotia*, 740 F.2d 817 (11th Cir. 1984). In practice, however, this does not happen. Because such subpoenas may in a handful of cases adversely affect relationships with other countries, current DOJ policy has curbed its own authority and prohibits prosecutors from using so-called *Bank of Nova Scotia* subpoenas unless DOJ's Office of International Affairs (OIA) has approved their use. And OIA rarely, if ever, approves their use, viewing them as a "last-resort" option where cooperation with a foreign government is not feasible, a conclusion that can take years to reach -- while the records often become obsolete in the meantime.

Under DOJ policy, to access such records law enforcement must instead rely on Mutual Legal Assistance Treaties (MLATs) with foreign countries. The terms of such agreements vary, but generally allow U.S. law enforcement to request assistance from the foreign jurisdiction to obtain evidence. OIA oversees the MLAT request process for the U.S.

In practice, the antiquated MLAT process takes months and even years of bureaucratic maneuvering, even in the best-case scenario with cooperative partners on the other side eager to help each other. When we are dealing with an uncooperative country or one that has data protection or secrecy laws, we may not get any evidence at all. In less than two minutes, a money launderer with a smartphone can move illicit proceeds halfway across the world. But for the government, it might take months or even years to obtain evidence of the money flows, if ever. And by then it may be too late. Criminal proceeds are liquidated or moved to new accounts in other jurisdictions, and evidence of associations between individuals and companies become stale.

Although these delays get chalked up to working with foreign governments, part of the problem is a self-inflicted wound: it lies in the way DOJ processes MLATs, a process designed long before so much evidence had gone both digital and global. This is illustrated by examples in cases I prosecuted. In one high-profile public corruption investigation, a foreign entity was ready to hand over evidence that included financial records to our investigative team. We needed those records to proceed further in the investigation. The FBI had a local attaché and a friendly relationship with local law enforcement, and we had a third-party custodian willing to voluntarily disclose records. But a highly bureaucratic process nonetheless ensued.

I drafted a memo and MLAT request to OIA. It was assigned to the OIA representative in Washington responsible for that country for review and some time later I received stylistic comments. After incorporating those, I had to send it back to Washington for several more layers of OIA supervisory review. This led to more comments requiring incorporation. This back and forth alone took weeks if not months. We assumed after this our MLAT was physically with our foreign counterparts who were eager to share records that were material to our investigation. Instead some time later OIA sent us a form to complete concerning which DOJ component was going to pay for the MLAT translation, meaning that it had not even left DOJ. Being a government contract, not just any translator can perform this task and if "expedited" translation of 30 days or less is desired, one must write an additional justification memo requiring its own layers of bureaucratic approval. The bottom line is that by the time we got our evidence it was approximately six months later, and this was in a case where there was no dispute with the foreign government over the provision of records.[2] With a subpoena, records like that could be obtained within weeks instead of months or years.

In another case against a major cybercrime ring, many months elapsed from the time we drafted MLATs seeking international bank records to the time the MLATs were actually *sent* to several receptive jurisdictions. Yet the time it took to get the records back from those jurisdictions was much shorter. Had we not experienced months of needless delay, we may have been able to put the case together sooner, apprehending these individuals before they committed further crimes and depleted some of the subject bank accounts. And in a high-profile money laundering case to a friendly European jurisdiction, a fellow prosecutor's MLAT request seeking records sat within DOJ for over a year.

Unfortunately, these examples are not outliers. These are actually the good news stories where records were eventually obtained and we were able to bring charges. And these were in cases DOJ considered high profile. Imagine a case involving more routine transnational criminal conduct, where there is no attaché to help shepherd the MLAT through, or worse still, the host country is not receptive or has no MLAT treaty. In such cases, records may never be obtained at all. In one well known international organized crime case prosecutors lost the ability to bring certain charges because the MLAT took too long. In other cases, bank accounts

[2] Although this statistic is anecdotal, a senior DOJ official told me that there was a backlog of approximately 13,000 MLAT requests at the time this particular MLAT request was pending.

were emptied before records requested via MLAT were produced. Prosecutors are conditioned to expect a basic MLAT in a friendly jurisdiction to take many months, and years in a non-friendly jurisdiction, a fact that deters some from investigating cases that will require them in the first place.

What causes the delays? *First*, there were too many layers of bureaucratic review in every case.[3] *Second*, those responsible for making decisions about the collection of overseas evidence are not part of the team responsible for the case, yet they are making decisions essential to the case. Add to this that OIA is responsible not only for outgoing MLATs from U.S. law enforcement, but also for incoming MLATs from foreign law enforcement.[4] *Third*, there is no tracking system to show where or with whom the MLAT resides at any given point. DOJ has acknowledged it lacks any means of monitoring MLATs, including transparency for monitoring "the progress of each request at each iterative step," and there is no system for MLAT partners to monitor the status of requests. *See* DOJ, Criminal Division FY 2016, President's Budget at 22-25. Although addressing these factors would certainly not mean evidence would be obtained from foreign authorities overnight, it would go a long way toward expediting the process and in fast-moving investigations every day can count. I need to stress here that the problem is with the OIA process and not the personnel.

And the problem is not confined to cybercrime investigations; it impacts cases involving trafficking in narcotics, weapons, and people; fraud; terrorist finance; public corruption; and really any crime that involves the movement of money. It arose in the investigation into the Russian election probe: it was widely reported that Mueller's team subpoenaed foreign bank records in the case against Paul Manafort. If Mueller's team had gone through the process described above instead of subpoenaed the banks directly, would the evidence have been timely obtained? By not using *Bank of Nova Scotia* to full effect and requiring its own internal bureaucracy, U.S. law enforcement is tying one hand behind its back in the fight against global money laundering.

Reaffirming law enforcement's authority to obtain records directly from a foreign bank's U.S. branch or correspondent bank could bring about a much-needed change in investigations, because it would allow U.S. law enforcement to more quickly and effectively track movement of funds without going through the cumbersome process described above. The question arises

[3] It may be that some complicated requests merit more review, particularly where the vagaries of foreign law require it, but the routine requests appear to needlessly go through much the same bureaucratic and time-consuming review process.

[4] Many foreign law enforcement partners prioritize U.S. MLAT requests given that our foreign counterparts rely heavily on evidence stored in the U.S. for their own cases (from Google, Facebook, Twitter, Apple, etc.) and hope that prioritizing U.S. requests will expedite their own requests. However, the flip side of this is when our own bureaucracy delays the processing of incoming MLAT requests from other countries, those jurisdictions may "penalize" the U.S. by holding back evidence our MLATs seek.

as to where a foreign bank operates in jurisdictions with strict data privacy or bank secrecy laws. Such scenarios pose complex conflict of laws questions. But federal courts have reasoned where commercial transactions are international, conflicts are inevitable and U.S. criminal investigations cannot be thwarted whenever there is a potential conflict. *See, e.g. Nova Scotia*, *supra*. Other courts have reasoned that banks electing to do business in numerous foreign host countries have accepted the risk of inconsistent government actions, and that if a bank cannot "serve two masters and comply with the lawful requirements of [both countries], perhaps it should surrender to one sovereign or the other the privileges received therefrom." *See, e.g., First National City Bank of New York v. IRS,* 271 F.2d 616, 620 (2d Cir. 1959).

Passing Section 15 provides DOJ an opportunity to revisit its existing policy, and makes clear to the Executive and Judicial branches that Congress has considered the potential for conflicts and has resolved that in favor of law enforcement's ability to timely gather critical evidence. DOJ could extend its existing policy such that OIA approval would still be required for foreign bank subpoenas, thereby rendering Section 15 toothless.[5] To account for that possibility, the Committee may wish to include language requiring an annual report from DOJ concerning (1) the number of requests from law enforcement for foreign bank subpoenas; (2) the number granted; (3) the timeframe in which requests were resolved from the date first received; and (4) whether any categories exist for which OIA could grant ex ante blanket approval for foreign bank subpoenas, e.g., if law enforcement certified they believed absent the records funds were in danger of moving before an MLAT could be completed, whether certain banks or countries could be whitelisted, etc.

And regardless of Section 15 and its implementation, the MLAT process must be modernized and streamlined if law enforcement is to keep up with the those committing illegal acts. The Committee may therefore wish to request DOJ report on ways to modernize the MLAT process. Such a report may include the feasibility of an MLAT tracking system, in the same way that several other criminal matters are tracked within DOJ and in the same way that the Treasury Department tracks similar requests for international assistance; measuring what priority is being given to outgoing MLATs versus incoming MLATs; and providing statistics on the number of MLAT requests received, the time until fulfillment, etc.

A word on authentication. The provision requires foreign banks to produce *certified* records in response to the subpoena. At the investigative stage, financial records in any form are critical. Certified copies may become important if a case goes to trial, but given that over 90% of federal cases settle and most defendants waive Speedy Trial Act requirements, I view this provision as helpful though far less important than getting the records in some form in the first place.

[5] Unfortunately the process for requesting OIA approval to subpoena foreign banks is similar to the MLAT process, and is subject to its own set of delays. Many prosecutors believe that requesting approval for a foreign bank subpoena is as long and cumbersome as a formal MLAT request.

SECTION 18

Although to many, global money laundering conjures up images of offshore Cayman Islands accounts or secret Swiss bank vaults, the fact is that the U.S. is one of the easiest places in the world to launder money. According to our Treasury Department, a staggering $300 billion is laundered in the U.S. every year. Our laws regarding shell and shelf companies and beneficial ownership of accounts are one reason why.

Although there is nothing illegal about setting up shell companies – many do so to appropriately protect privacy and limit liability – plenty of others do so to conceal criminal activity and hide money. Fraudsters, cartels, terrorists, and corrupt officials do not want to keep stolen assets in their own names. They therefore create a company, or series of companies (including nested shell companies, or shells within shells), which can do all of the things they otherwise could have with their criminally-gotten proceeds: buy property, open bank accounts, and transfer money. In the U.S. and elsewhere it is easy and legal to create what are essentially anonymous companies. Lawyers, accountants, and other professionals derive substantial income from providing these services. And while shells are easy to set up, they make it difficult for investigators to link money with perpetrators.

The 2016 Panama Papers brought mainstream attention to the problem of concealing true beneficial owners of accounts. That leak revealed that a Panamanian law firm set up or managed offshore companies and hard-to-trace corporate structures for world leaders, drug kingpins, American fraudsters, and others. And 60 Minutes shed light on the role that U.S. lawyers play in helping criminals devise structures to launder money: An undercover investigator purporting to be an advisor to a West African minister met with lawyers from over a dozen New York law firms. He told them a story intentionally devised to raise red flags and lead them to believe he wanted to move tens of millions of dollars in payments from foreign companies (obtained using his official position in exchange for mineral rights) into U.S. real estate, a jet, and a yacht. Only 1 of 16 said no; most offered guidance on how it could be accomplished legally.

Parking money in accounts whose ownership is concealed has collateral consequences. It has been cited as fueling increased housing prices in cities like London, Miami, New York, Paris, Vancouver, and San Francisco, as western real estate holdings are a desired investment for dirty money. In fact, it was reported that in 2015 90% of new construction sales in Miami were in cash, a red flag for money laundering.[6] And according to the U.K.'s National Crime Agency, laundered money has skewed the London property market with overseas criminals

[6] *See* Miami Herald, "How Secret Offshore Money Helps Fuel Miami's Luxury Real-Estate Boom," April 3, 2016 at http://www.miamiherald.com/news/business/real-estate-news/article69248462.html.

sequestering funds there and driving real estate prices up 50% in less than a decade.[7]

To help combat the problem, the Treasury Department's Financial Crimes Enforcement Network last year announced the "Customer Due Diligence" beneficial ownership rule (CDD) which requires financial institutions to gather details about the individual(s) who *actually* owns or controls, directly or indirectly, an account held in the name of a legal entity like an LLC. The CDD will come into effect next May and is an important first step in the fight against international money laundering. But nothing in the CDD rule prevents individuals from simply lying about ownership to financial institutions, and financial institutions can rely upon customer representations. Section 18 would give the CDD teeth by making it a crime to provide false information to financial institutions concerning ownership or control of an account.

Many laypeople assume that is already a crime, but that is not always the case. For example, in 2012 we were investigating a group committing large scale mortgage fraud in California, a scheme that caused tens of millions of dollars in losses. The ringleader had bank accounts established in an acquaintance's name and paid the acquaintance, but the two agreed it was the defendant who would actually own the accounts. The defendant used this nominee account to facilitate his scheme, depositing mortgage fraud proceeds into it. We wanted to charge the defendant (or acquaintance) with lying to the bank about the account's true owner but realized this on its own was not a crime.[8] Prosecutors frequently see shell companies and corresponding financial accounts created to park foreign funds from overseas criminal activity, including from Russia and China. A group of Russian cybercriminals I prosecuted made extensive use of nominee accounts in the U.S. and Europe, yet we lacked charges to prosecute those who established the accounts. And a pair of corrupt federal agents on the Silk Road task force I prosecuted made use of shell companies and nominee accounts to conceal proceeds from their illegal activity. One of my former colleagues had a defendant whose sole occupation was to create shell companies, provide false identification documents as account holders, and move tens of millions of dollars across borders in furtherance of criminal activity.

Confronted with facts like these some prosecutors have gotten creative and charged such conduct as a violation of the bank fraud statute, 18 U.S.C. Section 1344. However, an element of that offense is that a defendant intended to defraud a financial institution – in other words the *financial institution* was the victim. But in many cases where someone falsifies information concerning financial account ownership for criminal activity, the financial institution is not the intended victim of the fraud; it may not lose any money and in some instances, may even benefit from the additional business.

---

[7] *See* Financial Times, "How Laundered Money Shapes London's Property Market," April 6, 2016 at https://www.ft.com/content/f454e3ec-fc02-11e5-b5f5-070dca6d0a0d.

[8] Because many of the mortgage lenders had gone out of business in the mortgage crisis, the records to charge mortgage fraud were not available to us for all transactions.

Thus, federal courts have split on whether it is permissible to charge a case of bank fraud where the financial institution was not the intended victim. Some courts of appeals have held that the financial institution itself must be the targeted victim for a bank fraud violation. *See, e.g. United States v. Thomas*, 315 F.3d 190, 197 (3rd Cir. 2002) ("the sine qua non of a bank fraud violation…is the intent to defraud *the bank*.") (emphasis added); *United States v. Blackmon*, 839 F.2d 900, 905-06 (2nd Cir. 1998); *United States v. Rodriguez*, 140 F.3d 163, 167 (2nd Cir. 1988) (schemes merely involving bank not crimes unless specific intent to victimize bank itself causing it to release property). Other courts have read the bank fraud statute more broadly, holding that deceiving a bank alone is sufficient and no intent to victimize the bank is required. *See, e.g., United States v. McNeil,* 320 F.3d 1034, 1037 (9th Cir. 2003) (requiring only that bank is in some way involved in the defendant's scheme); *United States v. Kenrick*, 221 F.3d 19, 26-29 (1st Cir. 2000). This split of authority means that whether such conduct is a crime under the bank fraud statute depends on what area of the country one is in.

I am aware of investigations where prosecutors struggle to find a statute to charge instances involving concealed beneficial ownership. They may be able to deploy other statutes to fit the conduct, they may not. But there is currently no clean, straightforward statute to charge this conduct. Section 18 would provide that. Criminal penalties could deter individuals, and importantly their agents, from lying about the ultimate owners of accounts. At the same time, it would ease the burden on financial institutions by putting part of the "know your customer" onus on the customer, who could be liable if they concealed, falsified, or misrepresented. Given how useful it is for criminals to have financial accounts that are seemingly unconnected to them, I view this feature of the legislation as an important next step in the fight against global money laundering.

Thank you for inviting me to share my thoughts on these important issues.