A Reckoning Looms for America's 50-Year Financial Surveillance System

Michael J. Casey

For all the upheaval of 2020, it's perhaps not surprising that the 50-year anniversary of a major piece of financial legislation came and went with little fanfare. But the 1970 U.S. Bank Secrecy Act (BSA) deserves much scrutiny.[1] In mandating that financial institutions maintain customer identity records and report illicit activity to government agencies, the BSA was a landmark statute by any measure. It paved the way to an ever-expanding system of international surveillance that's a cornerstone of U.S. economic power.

There have long been questions about whether this system, aimed at domestic and international money launderers, tax evaders, and other criminal financiers, provides a net benefit to global well-being. Its critics argue, for example, that the draconian rules excessively burden the poor, leaving billions excluded from vital financial services (de Koker 2006; Isern and de Koker 2009). Even so, in the years since the BSA's founding, the regime created in its wake has only become more pervasive.

Now, for the first time, a real alternative is emerging, courtesy of digital currency technology. This is empowering people, businesses,

---

Cato Journal, Vol. 41, No. 1 (Spring/Summer 2021). DOI:10.36009/CJ.41.2.14.

Michael J. Casey is Chief Content Officer at CoinDesk.

[1]For the full text of the Bank Secrecy Act (BSA 1970), also known as the "Currency and Foreign Transactions Reporting Act," see https://fraser.stlouisfed.org/title/bank-secrecy-act-1025.

and, most importantly, foreign governments to bypass intervention in their financial affairs. The situation poses a real threat to U.S. international power and creates avenues for other states, such as China, to boost their foreign influence. There is an urgent need to reassess U.S. regulatory priorities. Though rarely discussed, it is arguably the biggest of the many challenges facing President Joseph Biden.

A Leviathan Grows

Signed into law by President Richard Nixon and amended and expanded over time as concerns grew, first about international drug trafficking and, later, over terrorism, the BSA requires financial institutions to monitor and keep records of their clients' transactions, identities, and personal information. It obliges them to report total daily purchases of negotiable instruments exceeding $10,000 and to file suspicious activity reports (SARs) when transactions suggest potential money laundering, tax evasion, or other criminal activities. In the wake of the September 11 attacks of 2001, the BSA was amended under the USA PATRIOT Act. Since then, it has required the entities covered by the act to employ a pervasive identifying system known as "know your customer" (KYC) and to create formal anti-money-laundering (AML) programs with clear policies, procedures, and controls to put compliance officers in place, to hold ongoing employee training, and to conduct independent audits of the program. Those amendments also greatly expanded the act's definition of "financial institution" to include nonbank entities such as securities broker-dealers, casinos, money-service businesses, and insurance companies.

The BSA's founding fostered a variety of related agencies at home and abroad that together formed an increasingly complex, pervasive financial surveillance network. The Financial Crimes Enforcement Network (FinCEN), founded in 1990, receives the customer reports that banks generate and turns them into actionable intelligence against money laundering and other illicit financial activity. Upon its founding, FinCEN joined the Financial Action Task Force (FATF), a multilateral body created by the Group of Seven nations the previous year amid growing concerns about the international drug trade. Five years later, FinCEN became a founding member of the international Egmont group of Financial Intelligent Units (FIUs), which in compliance with the FATF's guidelines, has enforced an

interlinking, cooperative, KYC-based international system of record-keeping and monitoring.

Over time, FinCEN rule updates and "guidance" have expanded the umbrella of AML-KYC principles. Since 1999, the agency has explicitly required operations deemed as money-service businesses (MSBs) to register with it (Treasury 1999: 4). In 2013, the increasing popularity of bitcoin and other cryptocurrencies led FinCEN to expand its definition of those MSBs to include businesses involved in exchanging what the agency called "virtual currencies" (Treasury 2013). Since then, it has tweaked and adjusted its rules to expand its oversight of the sector. And in consultation with its fellow FATF members, many of these rules have essentially been internationalized as other FIUs follow FinCEN's lead.

While the FATF and the Egmont group are set up as equal-weight deliberative bodies, this international alphabet soup of agencies and monitoring programs has evolved to become an indirect, but effective mechanism for the United States to exercise significant influence over foreign businesses and governments. For example, this authority to monitor and curtail financial flows affords Washington broad sanctioning power under the Office of Foreign Assets Control—which, along with FinCEN now falls under the U.S. Treasury's Office of Terrorism and Financial Intelligence—and it forces foreign companies to comply with other U.S. laws such as the anti-Cuba Helms-Burton Act. This unique power derives from the dollar's status as the world's reserve currency, which leaves non-U.S. banks wishing to conduct cross-border transactions no choice but to create correspondent banking relationships with U.S. banks—typically Wall Street–based money-center institutions. As institutional "customers," those foreign banks must comply with those U.S. banks' KYC requirements, which in turn means they too must make similar demands of the smaller domestic banks they deal with, dictating how *they* monitor *their* customers.

In this article, I will discuss whether this hierarchical system of KYC and KYCC (know your customer's customer) has delivered a net benefit in terms of criminals caught and lives saved and whether or not U.S. and international peacekeeping interests have ultimately been served by tracking terrorists' and other violent actors' funds. But even if we assume a positive effect, let's describe it for what it is: an *all-pervasive, globe-spanning surveillance system.* This is important when addressing legitimate concerns over China's invasion of

privacy as it rolls out a centrally controlled digital currency that has the potential, privacy advocates warn, to become a "panopticon." I say this not to grant Beijing's supporters a chance for "whataboutism," but to point out that with America's enemies and competitors actively building technologies that get around Washington's financial gatekeeping powers, its own moral standing can be challenged.

But Is It All Worth It?

So, after 50 years of the BSA, let's try to measure its effectiveness. Little is known about how much money laundering and illicit financial activity goes uncaught. After all, it's an immeasurable counterfactual. A 2011 UN Office on Drugs and Crime study estimated that in 2009, criminals laundered $1.6 trillion, or 2.7 percent of world GDP (UNODC 2011). (Tellingly, no international accounting of the problem has occurred in the decade since.) More recently, a trove of leaked FinCEN documents revealed that banks had flagged around $2 trillion worth of suspicious transactions to authorities between 1999 and 2017, and in many cases, they continued to do business with those entities (Leopold 2020). Many of those transactions were likely legitimate, and even for those recognized as illicit, there are often legitimate enforcement reasons for maintaining and monitoring these criminals' activities before shutting them down. Nonetheless, when combined with the UN report and other accounts of widespread financial fraud, the leaks are a reminder that for all this surveillance infrastructure, policing illicit money movements is extremely difficult. The global AML-KYC dragnet has gaping holes in it.

On the other hand, the system's pervasive identifying, tracking, and reporting of transactions imposes very real costs on the global economy. It adds friction to finance, hindering people's capacity to engage in exchange, especially in countries with underdeveloped record-keeping systems and excessive corruption, where IDs don't rise to U.S. banks' standards. Although lightweight mobile banking solutions and other initiatives helped lower the proportion of the world's adult population without a bank account from 49 percent in 2011 to 31 percent in 2018, some 1.7 billion adults still fell into the World Bank's "unbanked" category (Demirgü-Kunt et al. 2018). Amid the lifestyle constraints imposed by Covid-19 restrictions and

an aversion to using physical cash, a lack of access to online banking has since put these people at an even greater disadvantage.

Beyond mere access to a transactional bank account, financial services in general remain prohibitively expensive for far too many. In the United States itself, some 66 million adults, or 22 percent of the population, were considered "unbanked" or "underbanked" in 2018, according to the Federal Reserve (Federal Reserve 2019). Too few people of low income can obtain credit or other financial services because compliance-burdened banks find it unprofitable to service them. Even though the FATF recommends exemptions from customer reporting on transfers of less than $1,000 and the United States sets a threshold of $3,000, banks' strict application of KYC-AML rules across all customer and interbank relationships has fostered widespread risk aversion among bankers. Engaging with the poor is just not worth the risk for them. This has left billions of people in the world's informal economies as bystanders to the global economy and unable to break free of poverty.

Meanwhile, the bad guys that the laws are intended to catch find the means to get around them. They have all sorts of methods for obscuring money flows and identities through a maze of shell companies and complex netting and laundering procedures. There have long been bankers who are willing, for a fee, to turn a blind eye. And as shown by the Panama Papers revelations about the law firm Mossack Fonseca, services exist to actively create ownership and reporting structures that allow money of suspect origin to find a resting place in untouchable, offshore accounts (ICIJ 2016).

Beyond the moral inequity of the system, it can also be viewed as a barrier to self-determination in non-U.S. jurisdictions, breeding anti-American sentiment—often among the kinds of people the United States should be cultivating. In 2014, I met a small group of young bitcoin entrepreneurs in Hong Kong, some of whom would a few years later use their technology to help anti-Beijing student protesters avoid surveillance by authorities. Each told me their biggest hurdle lay in opening a company bank account. Their local banks had told them they held no concerns of their own about cryptocurrency service providers but that their U.S. subsidiaries worried about meeting their U.S. banking counterparts' compliance demands and that they might look unfavorably on a Hong Kong sister institution dealing with this little-understood industry. With the Sword of Damocles hanging over bankers' heads, these entrepreneurs had become

victims of a fear of what *might* happen. It's a system of control by uncertainty.

Entire countries and regions have been ravaged by this financial "de-risking" trend, which grew as regulations tightened after, first, the September 11 attacks in 2001, and, later, the financial crisis of 2008. Expanded AML-KYC regimes have seen U.S. banks pull back on lending or on processing payments to and from banks in small foreign economies because the compliance costs and legal risks outweigh the payoff from doing business on a small scale. A 2017 survey by the Caribbean Association of Banks found that 21 of 23 banks in 12 countries had lost at least one correspondent banking relationship (De Souza 2017). The upshot is that the cost of credit and of sending and receiving money has risen for Caribbean islanders even as their countries' offshore banking and insurance industries have welcomed massive financial inflows from foreign institutions. It's a tale of two entirely divergent island economies, their divisions accentuated by fallout from U.S. laws—one a purely legal construct for foreign corporations to exploit, the other a real-world community of striving human beings.

In these and other ways, America's obsession with financial snooping erects barriers around the world, hindering the ability of entrepreneurs of all sizes to innovate and bring valuable new ideas and businesses to market. The opportunity cost of all of that missed production and progress is incalculable. And while financial regulators would have us believe it's the price we must pay for staying safe, the view from 2021 makes it hard to see anything but a terrible deal. What solutions to the world's mounting challenges might have arisen if it weren't too expensive for so many people to build them? What acts of violence, crime, or terrorism might never have occurred if their perpetrators didn't find fertile recruiting grounds among the desperately poor who are cut off from remittances and other financial life bloods?

Despite all these barriers, one extremely important innovation has broken through them to pose a serious disruptive threat to this U.S.-centric financial surveillance regime. Cryptocurrencies and blockchains, which have also spawned new ideas in traditional fiat money such as central bank digital currencies (CBDCs) and "stablecoins," enable direct peer-to-peer transfers. They have the potential to bypass the surveillance system's gatekeeping institutions. They also portend a very real, geopolitical battle. President Biden will have to confront the challenge. Dealing with it will require some

outside-the-box thinking and a willingness to give up on some, if not all, of that gatekeeping power.

Toward Greenback Obsolescence

For now, much of the governments' attention on new financial technology's supposed threat to security has focused on decentralized cryptocurrencies such as bitcoin. They justify their concerns on frequent headlines about criminal enterprises using cryptocurrencies to move money around undetected. We recently heard European Central Bank President Christine Lagarde decry bitcoin's "funny business" and "reprehensible money laundering" trends (Reuters 2020). Citing similar concerns, India and Nigeria recently moved to ban cryptocurrencies outright (De 2021a). And in late December 2020, outgoing Treasury Secretary Steven Mnuchin delivered a draconian anti-crypto proposal at the 11th hour of the Trump administration (De and Nelson 2020). It would require cryptocurrency custodial businesses such as exchanges and hosted wallet providers to not only report their own customers' identities to FinCEN but also those of the third-party holders of so-called self-custody wallets with whom those customers often transact. The proposal, which had its public comment period extended twice such that it now closes March 29, had by late-February attracted a record 7,500 comments. A great many were critical, calling it a barrier to innovation, a breach of people's right to privacy, and a blow to the liberating potential that such wallets offer to people living under authoritarian regimes in China, Venezuela, Iran, or other such places.

Even setting aside these powerful civil liberty arguments, there are two big problems with regulators' kneejerk anti-crypto posture. The first is that while it's true that bitcoin is used by criminals, who need not provide identifying information when moving money between self-hosted wallets, innovative regulators in some jurisdictions are equally finding they can use the system to monitor flows and aid enforcement. Even though transaction data is pseudonymous, the system's permanent, public blockchain ledger means payments can be easily traced from origin to exit point. Criminals are seeking out technologies that obscure those flows, but savvy enforcement agents are right there with them, using similar disguising technology to infiltrate these illicit networks and break them up. Recent successes in

using blockchain technology to trace criminal interactions and apprehend perpetrators include the arrests of participants in the mid-2020 Twitter hack (Chainalysis 2020). The jury is still out on whether, on balance, bitcoin hinders police work or actually aids it.

The second big problem with this cryptocurrency obsession is that it leaves regulators blind to a far bigger technological challenge to their enforcement model: the one being developed by governments. Different countries will soon easily build interoperability across their respective central bank digital currencies' protocols (BIS 2020: 7) so that a user of one CBDC, such as a Russian importer, can directly transfer value to someone using the other, such as a Chinese exporter. This creates a secure cryptographic information channel that negates the need for the current cumbersome, bank-led model run by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Also, if they employed a blockchain-based escrow system that neither party could manipulate, the importer and exporter could establish a smart contract that protects both sides from currency volatility without needing to protect their positions via an intermediating reserve currency such as the dollar (Casey 2019). We could soon see the intermediation of correspondent banks all but removed from global commerce, saving trillions of dollars in financial fees.

China, the United States' main economic rival, is well ahead of pretty much every country in developing CBDC technology, with its Digital Currency and Electronic Payments (DCEP) system now rolling out. While the DCEP project is currently focused on domestic retail use cases, its forthcoming integration into decentralized supply chain solutions and other blockchain systems with the potential to cross borders has broad international implications. China could leverage its deep investments in Africa, for example, where Chinese technology lies at the heart of the continent's information infrastructure to seed widespread use of the digital yuan there. And among the 65 countries within the Chinese-sponsored Belt and Road project, at least one is already signaling interest in developing interoperability capacity with the DCEP. (During a World Economic Forum panel discussion that I moderated in January, Singapore Senior Minister Tharman Shanmugaratnam indicated as much in an exchange with Zhu Min, a former People's Bank of China governor and deputy managing director of the IMF who is now chairman of China's National Institute of Financial Research.)

All this will be game changing for the United States, which as we've described has built a model of surveillance and power around its dominance of international banking. For now, it might seem the dollar is stronger than ever, given the surging demand for greenbacks unleashed by the Covid-19 crisis and the Federal Reserve's willingness to act as the world's liquidity provider of last resort. But in reality, the international imbalances fostered by this global dependency, which has generated massive dollar-denominated bank assets and liabilities in Europe and Asia, is stirring talk in international circles about how digital currencies might help the world exit the dollar standard.

In a bombshell speech at the Federal Reserve's annual Jackson Hole conference in 2019, for example, former Bank of England Governor Mark Carney proposed a new multilateral digital currency to replace the dollar (Carney 2019). Many others believe we are more likely to move to a less orderly, multicurrency world of interoperable CBDCs and cryptocurrencies, one that no longer needs the U.S. banking system (see Birch 2020; 187–215). Either way, both scenarios spell the end of what former French Finance Minister Valéry Giscard d'Estaing once described as America's "exorbitant privilege" (Eichengreen 2010: 4).

Biden's Moment

What is the Biden administration to do about this? Well, the first thing needed is awareness. Thankfully, the new president appears to be building on some of the Trump administration's more change-embracing approaches to this field while adding expertise to areas where it was lacking. Christopher Brummer, Biden's pick for chairman of the Commodity Futures Trading Commission (CFTC), is a fintech specialist whose knowledge of cryptocurrencies and other disruptive financial technologies suggests a continuation of the CFTC's recently acquired reputation as Washington's most innovation-friendly regulatory agency.

Meanwhile, the Biden administration might drive a more forward-looking position among some of the Trump era's more reactionary factions. New Treasury Secretary Yellen has cautiously recognized cryptocurrencies' potential to "improve the efficiency of the financial system," offering a contrast to Mnuchin, who industry insiders described as openly hostile to

the crypto industry (De 2021b). There's also real hope that Gary Gensler, the new chairman of the Securities and Exchange Commission, will soften Jay Clayton's heavy-handed opposition to cryptocurrency exchange-traded funds and will generally take a more pro-innovation view of the potential for cryptocurrencies to reduce rent seeking by intermediaries. Gensler, who served as chairman of the CFTC in President Obama's challenging first term, spent the past few years teaching cryptocurrency and blockchain courses at MIT.[2]

It's noteworthy also that before his nomination, Gensler headed Biden's financial regulatory transition team, a group that included fellow MIT professor Simon Johnson, a former IMF chief economist who became a prominent critic of Wall Street's excessive powers during the financial crisis. As a founding member of MIT's Digital Currency Initiative (where I also worked), Johnson was instrumental in stoking Gensler's interest in this technology's potential. It's also worth noting that in November 2019, Gensler joined other leaders of past Democratic administrations, including former Treasury Secretary Lawrence Summers and former Defense Secretary Ash Carter, in a simulated "currency war game" at Harvard. The simulation explored how digital currencies might affect the United States' capacity to pursue its international interests. CoinDesk's Nikhilesh De captured the group's concerns in a summary of their hypothetical game scenarios: "China's central bank digital currency (CBDC) has undermined the dollar's dominance of the global financial system. North Korea has used the digital yuan to build and test nuclear missiles, safely evading financial sanctions imposed by Washington. And malicious actors are stealing funds from the SWIFT communications network to prove a point." (De 2019).

Openness is the Solution

Awareness is one thing. The bigger challenge is the policy response. To paraphrase Clayton Christensen, the new government faces the ultimate "innovator's dilemma" (Christensen 2016).

[2] Full disclosure: I co-wrote a paper on the potential and pitfalls of blockchain technology with Gensler and other MIT researchers during my tenure at that institution (see Casey et al. 2018).

For the United States to fully embrace the efficiency and competitive opportunities that digital currencies and related technologies offer the world economy, it must ultimately abandon the century-long hegemony afforded to it by the current system. This would mean giving up on the Federal Reserve's almost consequence-free capacity to print money, set low interest rates, prop up financial assets, and spur debt-fueled consumption. It would also mean surrendering the surveillance and political influence powers that arise from the gatekeeping dominance of U.S. banks. It would spell the end of Wall Street as a global powerhouse.

At the same time, doing nothing is a recipe for disaster. We can make analogies here to the fate of countless once-dominant industries that were disrupted by new technologies—from steam engines to video rental stores—although the stakes are magnitudes higher. Hemmingway's maxim about bankruptcy occurring in two ways—"first slowly, then all of a sudden"—seems apropos here. Once the world's business leaders realize they now have a programmable medium of exchange that allows them to lower the risk of transacting with each other without paying gatekeeping fees or submitting to the controls of American banks, the dollar will first slowly lose ground as a part of global commerce then suddenly drop to irrelevance. In the end, the United States will have no option but to cede the intoxicating power of the old regime and invest in generating as much benefit as possible from this new technology.

That might sound like the government is between a rock and a hard place. But there's another way to look at this, one more finely attuned to the traditional idea of American "soft power." If, as many a U.S. statesman has declared, the country's interests are best served by promoting open markets and free societies, then there is a big opportunity to seize the moral high ground in the battle for the future of money. The best way to conceive of that is to think of the dilemma the authoritarian Chinese President Xi Jinping faces with regard to the privacy and transactional freedom of his countrymen versus the more open position that the United States, at least ostensibly, is supposed to represent. By that idealistic standard, at least, President Biden has less of a dilemma and more of an opportunity.

Former CFTC Chairman Christopher Giancarlo has founded his Digital Dollar Foundation on this very idea. He argues that the U.S. Constitution's embedded privacy protections would give a

future digital dollar a powerful advantage over both the digital Chinese yuan, which is burdened with state surveillance, and the Facebook-founded Diem project (formerly known as Libra), where users fear commercial surveillance (Giancarlo 2020). The counterpoint to this, of course, is that for the past 50 years, as we've discussed, the United States has been surveilling everyone's transactions. And more recently, as Edward Snowden's revelations revealed, it has shown a deep willingness and capacity to apply that to our internet transactions, be they monetary or otherwise. Admirably, the Digital Dollar Foundation's prototype for a digital dollar deliberately limits such interventionist state powers. But for a new monetary model to truly serve U.S. global interests, it must take an even more pro-innovation posture than merely creating a digital dollar. For inspiration, we can look to the openness principles that drove the first round of internet regulation under the Telecommunications Act of 1996 (FCC 2013).

At that time, in a moment of unique, post–Cold War American power, the logic of U.S. interests in the expansion of disruptive internet technology was clear: open everything up. You saw it in the move to force the regional Baby Bell telecom companies to provide access to their existing telephone wires to startup digital competitors. You saw it in the United States giving support to multi-stakeholder transnational institutions such as ICANN and the IETF to govern disputes over internet real estate in ways that contained vested interests. And you saw it in then Federal Communications Commission Chairman Reed Hundt's trips abroad, where he actively sold the idea that if other countries would adopt a similarly laissez-faire approach to internet startups and access to infrastructure, we'd all be better off.

That was a moment of consummate American power, wrapped in a proactive internationalist agenda, when there was a clear view that big opportunities would arise if free trade and open development were allowed to flourish. It paved the way for a new, internet breed of U.S. corporate behemoths in Amazon, Facebook, and Google.

Cryptocurrency technology is the next decentralizing phase of the internet, in this case attacking the gatekeeping powers of both Wall Street and the aforementioned post-1996 internet titans. As such, it offers a similar American opportunity as the one that arose 25 years ago, with even more potential to disrupt the political status quo. Rather than simply creating another digital dollar in the hope the world will fall for the myth of its superior privacy protec-

tions, Biden's Washington needs to find some of its Clinton era groove and set an international example for openness. That means taking a more proactive, less constraining approach to regulation so that new forms of decentralized and private cryptocurrency and stablecoin payments can arise and compete with each other, and with the dollar itself. The Chinese Communist Party government, with its capital controls and its "social score" system for surveilling its citizens, simply can't afford to promote such a model. If open-system alternatives exist with American backing, it's hard to see how a digital yuan could compete.

Conclusion

If the United States were to treat money less as a means of controlling everyone and more as a field of opportunity for creative start-ups to provide channels of creativity and financial access for billions of excluded people, we might just get to live through another American century. Sure, there'd be no more Wall Street, and Silicon Valley would see its piece of the rapidly expanding global innovation pie shrink. But in the place of that international dominance would come the ultimate victory: a global financial system built on core American values that burnish free societies and breed prosperity worldwide.

References

Birch, D. G. W. (2020) *The Currency Cold War: Cash and Cryptography, Hash Rates and Hegemony*. London: London Publishing Partnership: 187–215.

BIS (2020) "Central Bank Digital Currencies: Foundational Principles and Core Features." Bank of International Settlements. Available at www.bis.org/publ/othp33.pdf.

BSA (1970) "Bank Secrecy Act." Federal Reserve Bank of St. Louis, Fraser: https://fraser.stlouisfed.org/title/bank-secrecy-act-1025.

Carney, M. (2019) "The Growing Challenges for Monetary Policy in the Current International Monetary and Financial System." Speech given at "Challenges for Monetary Policy," a symposium sponsored by the Federal Reserve Bank of Kansas City, Jackson Hole, Wyoming (August 23). Available at www.bis.org/review/r190827b.htm.

Casey, M. J. (2019) "A Crypto Fix for a Broken International Monetary System." CoinDesk. Available at www.coindesk.com/a-crypto-fix-for-a-broken-international-monetary-system.

Casey, M. J.; Crane, J.; Gensler, G.; Johnson, S.; and Nurala, N. (2018) "The Impact of Blockchain Technology on Finance: A Catalyst for Change." *Geneva Reports on the World Economy* 21. The International Center for Monetary and Banking Studies. Available at www.sipotra.it/wp-content/uploads/2018/07/The-Impact-of-Blockchain-Technology-on-Finance-A-Catalyst-for-Change.pdf.

Chainalysis (2020) "Chainalysis in Action: How Law Enforcement Used Blockchain Analysis to Follow Funds and Identify the Twitter Hackers." *Chainalysis Blog*. Available at https://blog.chainalysis.com/reports/chainalysis-doj-twitter-hack-2020.

Christensen, C. (2016) *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail.* Cambridge, Mass.: Harvard Business Review Press.

de Koker, L. (2006) "Money Laundering Control and Suppression of Financing of Terrorism: Some Thoughts on the Impact of Customer Due Diligence Measures on Financial Exclusion." *Journal of Financial Crime* 13 (1): 26–50.

De, N. (2019) "In Wargaming Exercise, a Digital Yuan Neuters U.S. Sanctions and North Korea Buys Nukes." CoinDesk. Available at www.coindesk.com/in-wargaming-exercise-a-digital-yuan-neuters-us-sanctions-and-north-korea-buys-nukes.

_____ De, N. (2021a) "Janet Yellen Offers US Senate a More Nuanced Take on Crypto," CoinDesk. Available at www.coindesk.com/janet-yellen-offers-senate-a-more-nuanced-take-on-crypto.

_____ (2021b) "State of Crypto: India and Nigeria's Crypto Crackdowns Continue Old Trends." CoinDesk. Available at www.coindesk.com/india-and-nigerias-crypto-crackdowns-continue-old-trends.

De, N., and Nelson, N. (2020) "US Floats Long-Dreaded Plan to Make Crypto Exchanges Identify Personal Wallets." CoinDesk. Available at www.coindesk.com/fincen-proposes-kyc-rules-for-crypto-wallets.

Demirgü-Kunt, A.; Klapper, L.; Singer, D.; Ansar, S.; and Hess, J. (2018) "The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution." World Bank Group 19–22.

Available at https://openknowledge.worldbank.org/handle/10986/29510.

De Souza, I. (2017) "Correspondent Banking and De-Rrisking in the Caribbean." Caribbean Association of Banks. Available at http://cab-inc.com/wp-content/uploads/2016/07/Correspondent_Banking_and_Derisking_IDS_3.docx.

Eichengreen, B. (2010) *Exorbitant Privilege: The Rise and Fall of the Dollar and the Future of the International Monetary System*. Oxford: Oxford University Press.

FCC (2013) "Telecommunications Act of 1996." Available at www.fcc.gov/general/telecommunications-act-1996.

Federal Reserve (2019) "Report on the Economic Well-Being of U.S. Households in 2018." Available at www.federalreserve.gov/publications/2019-economic-well-being-of-us-households-in-2018-banking-and-credit.htm.

Giancarlo, C. (2020) "The Digitization of Money and Payments." Testimony before the U.S. Senate Committee on Banking, Housing and Urban Affairs. Available at www.banking.senate.gov/imo/media/doc/Giancarlo%20Testimony%206-30-20.pdf.

ICIJ (2016) "The Panama Papers: Exposing the Rogue Offshore Finance Industry." Available at www.icij.org/investigations/panama-papers.

Isern, J., and de Koker, L. (2009) "AML/CFT: Strengthening Financial Inclusion and Integrity." *CGAP Focus Note* 52.

Leopold, J. (2020) "The FinCEN Files." Buzzfeed News. Available at www.buzzfeednews.com/article/jasonleopold/fincen-files-financial-scandal-criminal-networks.

Reuters Staff (2020) "ECB's Lagarde Calls for Regulating Bitcoin's 'Funny business.'" Reuters. Available at www.reuters.com/article/us-crypto-currency-ecb/ecbs-lagarde-calls-for-regulating-bitcoins-funny-business-idUSKBN29I1B1.

Treasury Department, FinCEN (1999) "Amendment to the Bank Secrecy Act Regulations: Definitions Relating to, and Registration of, Money Services Businesses. 31 CFR Part 103 RIN 1506–AA09." *Federal Register* 64.

_____ (2013) "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies." FIN-2013-G001. Available at www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

UNODC (2011) "Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes: Research Report." Available at www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.