THE REVIEW OF
BANKING & FINANCIAL SERVICES
A PERIODIC REVIEW OF SPECIAL LEGAL DEVELOPMENTS AFFECTING LENDING AND OTHER FINANCIAL INSTITUTIONS

Vol. 32 No. 10 October 2016

SANCTIONS-RELATED CHALLENGES FOR PAYMENTS SYSTEMS

The rapid evolution of the payments industry — in particular the rise of non-bank actors and mobile computing — has created immense compliance challenges and risks for both the industry and regulators. The author discusses the regulators' intensified sanctions and AML enforcement efforts, the OFAC risk matrix, and its use as a reference source for compliance managers and counsel. He then turns to the burdens and benefits of the multiplicity of regulators. He closes with PayPal's proposed new approach to "KYC."

By Thomas Feddo *

There have been many consequences stemming from the September 11, 2001, terrorist attacks on the United States. One of them — the "whole-of-government" response to the challenges of terrorism and to widespread unrest around the world — has led to the development of a sprawling, global intelligence effort, the rise of the national security complex, and the unparalleled use of economic sanctions to target the financial resources of terrorist organizations, their state sponsors, and regimes bent on acquiring weapons of mass destruction (WMD). The burgeoning global payments industry has become a collateral target of the government's economic sanctions efforts, and it faces real challenges going forward.

Today's U.S. economic sanctions programs are exceptionally diverse and complex, creating dynamic and resource-intensive regulatory compliance requirements for financial institutions and companies alike. The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) implements and enforces over 30 different sanctions programs, each of them unique and tailored to achieve specific foreign policy objectives. Many sanctions can be extraterritorial in reach, crossing foreign jurisdictions with the same ease as the digital value transfers they seek to impede and disrupt.

HOW DID WE GET HERE? THE "SEPTEMBER 12" MINDSET

Economic sanctions have in many ways become a default foreign policy tool in responding to developing or worsening national security challenges around the world. From 2006 to 2010, the president issued 16 executive orders related to economic sanctions, but in the following five years that number more than doubled to 33. Nearly simultaneously, and not unrelatedly, economic sanctions have witnessed increasing

* *TOM FEDDO is a partner in Alston & Bird's International Trade & Regulatory Group in Washington, D.C. He counsels clients in the areas of U.S. economic sanctions, congressional investigations, and a variety of national security matters. Previously, he served as the assistant director for enforcement at the Office of Foreign Assets Control (OFAC). His e-mail addess is thomas.feddo@alston.com.*

IN THIS ISSUE

RSCR Publications LLC Published 12 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $650 per year in U.S., Canada, and Mexico; $695 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call (937) 387-0473 or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail shimmelfarb@comcast.net. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 1051-1741.

legislative involvement from the U.S. Congress, which has mandated certain actions by the executive branch, or promoted the development and implementation of powerful new sanctions tools, such as what is commonly referred to as "secondary sanctions."

In concert with the rapid creation and implementation of new sanctions programs, OFAC, the U.S. Department of Justice, New York State's Department of Financial Services, and other law enforcement authorities have intensified their sanctions enforcement efforts. The enactment of the International Emergency Economic Powers Enhancement Act of 2007 amplified the statutory maximum civil monetary penalty for a sanctions violation to *the greater of* $250,000 or twice the value of the underlying transaction. In the years since, the size of civil monetary penalties and settlements has grown exponentially. From fiscal year 2011 through fiscal year 2015, OFAC's civil monetary penalties or settlements alone have totaled more than $2.8 billion, and during the same period OFAC's median penalty increased by more than 600 percent. In fiscal year 2015, OFAC's mean monetary penalty or settlement was approximately $19.4 million.[1]

While the United States has sought through sanctions to disrupt terrorist financing and WMD development, the rapid evolution of the payments industry — in particular the rise of non-bank actors and mobile computing — has created immense challenges for both the industry and regulators. As regulators try to adapt and catch up, traditional financial institutions that already face heavy government scrutiny are currently bearing the brunt of the government's actions. Processing massive numbers of global, cross-currency transactions at nearly the speed of light, OFAC and anti-money laundering (AML) compliance is both a complicated and resource-intensive task. For example, a large money service business can spend upwards of $200 million annually screening for suspicious activity, and some of the largest financial institutions devote several thousand employees to AML and sanctions compliance. Financial institutions dedicate resources of this magnitude because of the serious risks that money laundering and terror financing can inflict on their operations, legal liability, and reputation.[2]

"FINTECH" INNOVATION AND DISRUPTION HAPPENING AT LIGHT SPEED

The payments industry has likewise experienced — and continues to undergo — a profound period of rapid transformation and innovation. A confluence of technological developments and growing market demand has resulted in "increasing access to market infrastructure" and the making of "new regulated payment service providers."[3] Thus, a wide landscape of diverse and creative methods and brands are available for businesses or consumers to transfer value to other individuals or entities, including online and mobile payments, virtual wallets, stored value and encrypted cards, smartphone contactless payments, and virtual or digital currencies, among many others. According to the American Bankers Association, "the payments ecosystem is one of the most fertile sectors of innovation in the economy today. Banks and non-banks, established companies and garage-based start-ups, brick-and-mortar retailers and online pioneers — all are competing for the hearts, minds and wallets (literally and virtually) of the American consumer."[4]

Consumers of financial services now demand global, cross-border, cross-currency solutions. The World Bank has observed that "[p]ayment systems are moving from being a narrow channel for transferring funds to a much wider integrated network for transferring additional forms of value."[5] By one estimate, "well over 750

[1] Derived from OFAC's "Civil Penalties and Enforcement Information" tables (https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx).

[2] *21st Century Regulation: Putting Innovation at the Heart of Payments Regulation*, PayPal Company, October 28, 2013 (https://www.paypalobjects.com/webstatic/en_US/mktg/public-policy/PayPal-Payment-Regulations-Booklet-US.pdf) at p. 6.

[3] *Id.* at p. 8.

[4] *The Changing Face of the Payments System: A Policymaker's Guide to Important Issues*, American Bankers Association, 2013 (http://www.aba.com/Tools/Function/Payments/documents/2013EmergingPayments.pdf) at p. 11.

[5] *Payment Systems Worldwide: A Snapshot. Outcomes of the Global Payments Systems Survey 2010*, World Bank, 2010 (http://documents.worldbank.org/curated/en/2011/01/16422496/payment-systems-worldwide-snapshot-outcomes-global-payment-systems-survey-2010) at p. v.

payment systems [exist] throughout the world; systems that are constantly changing due to new technology or government regulation of the currency."[6] Global personal international transfers may exceed $600 billion in 2016,[7] and the United States is one of the largest senders of remittances globally, with U.S. immigrants in 2014 sending approximately $54 billion overseas.

As the demand rises — with an emphasis on cost, convenience, efficiency, and speed — many of these innovations and new payments platforms are being created and developed by the less regulated or unregulated non-bank, or "fintech," sector. Last year, according to the Office of the Comptroller of the Currency (OCC), "fintech companies in the United States and United Kingdom increased to more than 4,000, and investment in fintech companies since 2010 has surpassed $24 billion worldwide."[8] In 2015, the U.S. Department of the Treasury estimated that over 25 percent of U.S. households utilized non-bank financial institutions.[9] With these trends, sanctions and AML compliance risk exposure grows dramatically.

MOBILE, DIFFUSE, AND NON-TRANSPARENT PAYMENTS — CAN REGULATORS CATCH UP?

Considering the convergence of these two dynamic spheres — economic sanctions and fintech — the substantial challenges confronting payments systems in implementing effective sanctions compliance policies become evident. And while non-bank payment platforms are becoming key players in the global market, government regulators have not yet developed a sophisticated response to this new reality. The World Bank notes that the "traditionally dominant position of commercial banks over retail payment systems and services is being increasingly challenged by a variety of non-bank payment services providers. This translates into additional difficulties for payment systems overseers and regulatory authorities in defining and carrying out their policy goals in the area of retail payment systems."[10] And the American Banking Association has warned that "with numerous non-banks [now] involved with payments and storing payment account information, is there a regulator (or regulators) tasked with ensuring that they are also maintaining adequate safeguards or otherwise assisting in those government mandates? While many large non-bank organizations are likely to follow leading industry practices for securing payment information, there is no guarantee that that will be the case . . . [or] how such compliance would be assured through regulatory enforcement. . . . it is unclear if the same level of care will be practiced by smaller technology startups."[11]

Thus, given the rapidly developing technologies and numerous regulatory jurisdictions involved, transparency at all levels is elusive. For example, according to a 2010 World Bank survey, just over *half* of 139 surveyed countries legally required money service providers to fully disclose all transaction details before its execution.[12] Compliance may be patchy or inconsistent because, with so many new providers and technologies, there follows a natural uncertainty as to whether and what extent those new marketplace entrants are either required, or understand that they are required, to adhere to the same regulatory standards as more established or traditional market participants. When U.S. Senator Mark Warner at a Senate Banking Committee hearing recently asked Consumer Financial Protection Bureau (CFPB) Director Richard Cordray about enforcing regulatory standards in the context of market disruption and innovation, Cordray noted that "it would be not appropriate for new fintech startups to be getting an advantage in the marketplace because they are arbitraging the regulatory system, they are not complying, they are not taking seriously, or as seriously, what the banks and regulated institutions have to do."[13]

---

[6] *Fundamentals of Payment Systems*, Treasury Alliance Group LLC, 2014 (http://www.treasuryalliance.com/assets/publications/payments/Fundamentals_of_Payment_Systems.pdf) at p. 1.

[7] *Mobile Money/Global Money: An In-Depth Look at Modern Day Money Transfers*, Dr. Noel Maurer, November 19, 2015 (https://www.zenbanx.com/dms-can/Modern-Day-Money-Transfers-White-Paper.pdf) at p. 5.

[8] *Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective*, OCC, March 31, 2016 (http://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/pub-responsible-innovation-banking-system-occ-perspective.pdf) at p. 3.

[9] *National Money Laundering Risk Assessment*, U.S. Department of the Treasury, June 12, 2015 (https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf).

[10] *Payment Systems Worldwide: A Snapshot*, *supra* note 5 at p. xii.

[11] *The Changing Face of the Payments System: A Policymaker's Guide to Important Issues*, *supra* note 4 at p. 8.

[12] *Payment Systems Worldwide: A Snapshot*, *supra* note 5 at p. x.

[13] U.S. Senate Committee on Banking, Housing and Urban Affairs, April 7, 2016 (Webcast of hearing: http://www.banking.senate.gov/public/index.cfm/hearings?ID=106BA9C4-9E02-4CF6-97F8-EEC458DB4D7C).

THE OFAC SANCTIONS HAMMER

While some payments industry competitors are perhaps not yet as well-regulated, from a practical standpoint all payments providers nonetheless face significant operational compliance risks in many of the same areas encountered by traditional financial institutions — fraud and consumer protection, data and cybersecurity, recordkeeping, terror finance, money laundering, and U.S. and foreign economic sanctions.

In terms of U.S. economic sanctions enforcement, the payments industry is on notice that OFAC is paying attention. From major credit card companies' receipt of "Findings of Violation" for failing to make required reports of "blocked property,"[14] to recent settlements with a major money service business and a global payments processor[15] — each for failures in transaction screening — OFAC is dedicating some of its limited enforcement resources to promoting heightened sanctions compliance by payments systems.

According to its Economic Sanctions Enforcement Guidelines (the "Guidelines"),[16] when OFAC penalizes a sanctions violation it gives either mitigating or aggravating weight to the quality of the violator's sanctions compliance program. When it issued the Guidelines in November 2009, OFAC emphasized that it would apply "risk-based" principles[17] in assessing a compliance program and included with the Guidelines a "risk matrix." The matrix focuses on a number of characteristics and flags as high-risk elements such as: "a large, fluctuating client base in an international environment . . . a large number of high-risk customers . . . overseas branches . . . a wide array of electronic products and services . . . [and] a high number of customer and non-customer funds transfers, including international funds transfers . . . ." While the payments industry has many of these hallmarks, the OFAC assessment is a holistic one that emphasizes the totality of the particular facts and circumstances.

CAN PAYMENTS SYSTEMS SURVIVE OFAC'S CROSSHAIRS?

The OCC has remarked that fintech has some unique advantages over traditional financial institutions, including the ability to "focus their energy and resources on a single opportunity" without the resource burdens of "legacy technology systems" or brick-and-mortar infrastructure.[18] Fintech "also may have specialized technical knowledge, experience, and skills with respect to emerging technology and trends." The critical concern that regulators have, however, is "the degree to which new participants in the payments space maintain adequate controls that facilitate overall payments system integrity . . . ."[19] Ultimately, a key to managing sanctions and AML compliance risk is "the requirement that the parties undertaking a transaction are who they say they are and that they are acting within their powers."[20]

Though somewhat dated, OFAC's risk matrix implies that an entity should consider its internal management culture and operations, offering that the following management and cultural characteristics tend to indicate higher compliance risk: (1) management failing to

---

[14] *Visa International Service Association*, Finding of Violation Web post, August 13, 2013 (OFAC reporting violations and weapons of mass destruction sanctions violations, resulting from the failure of written procedures) (https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20130809_visa.pdf); *MasterCard International*, Finding of Violation Web post, March 16, 2016 (OFAC reporting violations, weapons of mass destruction sanctions violations, and global terrorism sanctions violations, resulting from failures in internal controls) (https://www.treasury.gov/resource-center/sanctions/ CivPen/Documents/20160316_MasterCard.pdf).

[15] *First Data Resources, LLC*, settlement Web post, April 15, 2015 ($23,336 settlement for sanctions violations related to the Kingpin Act due to compliance program flaws, including failures in red flagging and screening system integrity outside manipulation) (https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20150415_first_data.pdf); *PayPal, Inc.*, settlement Web post, March 25, 2015 ($7.7 million settlement for sanctions violations related to weapons of mass destruction, terrorism, Iran, Sudan, and Cuba, due to screening failures) (https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20150325_paypal.pdf).

[16] 31 C.F.R. Part 501, App. A.

[17] The agency's public comments regarding compliance and enforcement continue to emphasize that U.S. persons should "implement appropriate controls, commensurate with their OFAC sanctions risk profile . . . ." *See, e.g.*, OFAC Crimea Notice, July 30, 2015 (agency advisory issued to warn about "obfuscation" practices being used to circumvent sanctions involving Crimea) (https://www.treasury.gov/resource-center/sanctions/Programs/Documents/crimea_advisory.pdf).

[18] *Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective*, *supra* note 9 at p. 4.

[19] *The Changing Face of the Payments System: A Policymaker's Guide to Important Issues*, *supra* note 4 at p. 4.

[20] *21st Century Regulation: Putting Innovation at the Heart of Payments Regulation*, *supra* note 2 at p. 6.

emphasize the importance of compliance; (2) the absence of compliance policies and procedures, and deficient information technology systems; (3) insufficient staffing or no relevant lines of accountability; (4) little or no training for relevant staff; (5) failing to focus compliance on high-risk areas; (6) no screening policy for transactions and new accounts, or for periodic review of existing accounts; (7) compliance systems that fail to adapt to changes to OFAC's SDN List;[21] (8) no independent testing; and (9) neglecting to have a corrective action plan for when mistakes happen.[22]

The matrix is *not* a compliance policy or program, but it should serve as a useful reference resource for compliance managers and counsel. At the very least, the payments industry can be confident that OFAC *will* assess a compliance program against these factors. So in the context of that matrix, fundamentals of a reliable program (not unlike those implemented by traditional banking entities) include: (1) written policies and procedures for manual review and escalation of sanctions alerts; (2) regular and formal training and quality assurance for relevant personnel, and for processes involved in manual review; (3) due diligence and oversight of intermediaries and strategic partners; and (4) appropriate procedures for handling and reporting blocked assets to OFAC.

An obvious challenge during a period of rapid disruption and innovation is ensuring that "old" compliance processes are keeping pace with vulnerabilities created by those changes and the expanded geography, and that compliance resources match the new risk profile. Key elements of a durable payments system compliance program might include: (1) point-of-sale data collection and validation; (2) real-time "in-flight" transaction screening; (3) a means for transaction suspension and manual review; (4) agile screening technology to process transaction and customer data involving multiple jurisdictions, languages, alphabets, and cultures; (5) specialized systems and processes for payments involving sanctioned jurisdictions; and (6) the ability to test, calibrate, and adapt to regulatory requirements and the risk environment.

TOO MANY REGULATORS?

Because of the various sanctions and AML/Patriot Act reporting requirements, "payments system providers have become important government partners in enforcing various federal laws meant to combat illegal money laundering, threats to our nation's cybersecurity, and other important policy initiatives."[23] Data reported to the U.S. Department of the Treasury by financial institutions complying with U.S. banking requirements is "shared with the IRS and about 380 regulators, intelligence agencies, and law-enforcement departments."[24]

One can sense some degree of a Wild West atmosphere in terms of regulatory oversight of the payments space. Multiple regulatory agencies exercise oversight and examination authority, including numerous state regulators, the CFPB, U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), IRS, OCC, the Federal Reserve, and others. One industry participant has noted that the "rate and pace of change are compromising the effectiveness of existing regulation and the regulatory process."[25] Money service businesses are regulated under the Bank Secrecy Act and are required to register with FinCEN, but most states also have registration and regulatory requirements, and their oversight agencies often supervise both banks and MSBs. Many foreign jurisdictions also require registration or licensing, and exercise oversight through their governments' central banks, financial intelligence units, or finance ministries.

A recent report by the Government Accountability Office (GAO), not specifically focused on the payments industry, described the fragmented and overlapping U.S. financial regulatory structure among multiple agencies. While these duplicative authorities and varying missions may, and do, lead to inefficient and inconsistent oversight, bureaucratic delays, and challenges to comprehensive risk oversight, the GAO noted several counterbalancing benefits — both U.S. regulators *and* market participants find that the structure fosters regulatory competition, which can generate regulatory innovation; provides checks and balances among

[21] OFAC's List of Specially Designated Nationals and Blocked Persons (https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx).

[22] *See* the Web-based version for a complete matrix (https://www.treasury.gov/resource-center/sanctions/Documents/matrix.pdf).

[23] *The Changing Face of the Payments System: A Policymaker's Guide to Important Issues*, *supra* note 4 at p. 4.

[24] *Losing Count: U.S. Terror Rules Drive Money Underground*, Wall Street Journal, March 30, 2016 (http://www.wsj.com/articles/losing-count-u-s-terror-rules-drive-money-underground-1459349211).

[25] *21st Century Regulation: Putting Innovation at the Heart of Payments Regulation*, *supra* note 2 at p. 13.

individual regulators; and "has resulted in diversity, inventiveness, and flexibility in the banking system, which are important for responding to changes in market share and in technology."[26]

There is some evidence supporting the notion that government agencies are in fact engaging with the industry in a proactive and responsive way. For example, the OCC has acknowledged that "both banks and non-banks suggested that the 'rules of the road' governing the development of innovative products and services are unclear," and that "[m]any non-banks . . . desire to understand regulatory requirements and the supervisory environment as they seek to expand their relationships with banks."[27]

On March 31, 2016, the OCC released guidance on how the agency intended to improve its "understand[ing of] trends and innovations in the financial services industry, as well as the evolving needs of consumers of financial services."[28] Furthermore, the OCC planned to "bring together banks, non-banks, and other stakeholders through a forum and a variety of workshops and meetings to discuss responsible innovation in the financial industry. . . . The OCC will work with agencies like the [CFPB] on innovations promoted by or affecting banks subject to OCC and CFPB supervision. . . . Such coordination gives banks greater confidence that regulators who share responsibilities will consider innovative ideas consistently."

On April 29, 2016, the Federal Financial Institutions Examination Council (FFIEC) published a new appendix to the FFIEC Information Technology Examination Handbook's Retail Payment Systems Booklet, addressing mobile financial services (MFS).[29] The Booklet is a component of the FFIEC Information Technology Examination Handbook, which "provides guidance to examiners, financial institutions, and technology service providers (TSPs) on identifying and controlling risks associated with retail payment systems and related banking activities." An upshot of giving this guidance to examiners regarding MFS is that the FFIEC has also provided payments systems providers some transparency in terms of compliance expectations.

Meanwhile, on May 11, 2016, FinCEN issued its final rule on customer due diligence requirements for certain financial institutions, including determining "beneficial ownership."[30] The new regulation, however, does not apply to non-bank money services businesses that do not meet the definition of "covered financial institution." With widespread banking industry concern about the resource demands and implementation challenges of the new rule, FinCEN gave a nod to intense feedback and extended the implementation period from one year to two.

A MAJOR INDUSTRY PLAYER OFFERS A NEW APPROACH TO KNOW YOUR CUSTOMER ("KYC")

Collaboration regarding how government regulates payments systems obviously implicates the industry's participants as well. As the innovators, no one better understands the technology, processes, and systems than they do. One in particular has brought a clear-eyed and proactive approach to these issues, including the KYC screening that is so important to sanctions and AML compliance. PayPal has proposed to work "with governments around the world" on a regulatory paradigm that focuses on "performance standards" rather than "design standards."

In late 2013, the company issued a document regarding regulatory innovation in the payments industry. PayPal commented that "no one questions the need to combat money laundering and fraud. There is disagreement, though, about how the existing regulatory process can be enhanced to better achieve these goals. Current payments regulations generally utilize rigid design standards . . . and a methodology that cannot iterate with rapid developments in industry."[31] According to PayPal, design standards of KYC regulation "force these innovative businesses to dedicate resources to the collection of data points that may not be relevant to the goals behind the regulation."

In the past, identity was established by "physical presence" or providing a "trusted document."

---

[26] *Financial Regulation: Complex and Fragmented Structure Could Be Streamlined to Improve Effectiveness*, GAO-16-175, General Accountability Office, February 2016 (http://www.gao.gov/products/GAO-16-175) at p. 13.

[27] *Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective*, *supra* note 9 at p. 3.

[28] *Id.*

[29] Appendix E defines MFS as "the products and services that a financial institution provides to its customers through mobile devices," such as financial services implemented and offered through SMS/text messaging, mobile sites and browsers, mobile applications, and wireless payment technologies (http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems/appendix-e-mobile-financial-services.aspx).

[30] 81 Fed. Reg. 29,398 (May 11, 2016).

[31] *21st Century Regulation: Putting Innovation at the Heart of Payments Regulation*, *supra* note 2 at p. 2.

Technology is "challenging existing notions of identity," and to "address the shortcomings of the current landscape . . . means creating regulation that is collaborative and iterative" and uses data analytics "to make regulatory decisions that keep pace with the rate that the market is developing." In the KYC context of assessing compliance risk, PayPal noted the limits of reviewing a name and address — that it neglects risk factors such as a party's relationship to any other party, and what is "normal behavior" for the transacting parties. PayPal observed that "modern payment services are looking at the entire electronic footprint of actors when determining identity. . . . [M]odern payments providers are constantly adjusting the data points gathered . . . and the algorithms that analyze the data."

Thus, PayPal has proposed "a shift towards a more agile, collaborative, and insightful regulatory process" that would allow regulated parties to "adopt innovative methodologies to achieve regulatory goals. For example, an actor might experiment with capturing mobile telephone numbers or customer e-mail addresses as identity proxies rather than name and address."

CONCLUSION

As one payments participant has stated, "[p]ayments are increasingly enabling cross border transactions that were never before possible."[32] Other stakeholders have commented that "the need and interest of individuals to find low cost ways of moving money between themselves" and "the desire for alternatives to conventional systems is strong and technology enables some truly elegant ways of meeting this demand. The future is likely to see additional developments and variations to address the issues and opportunities inherent in alternative systems."[33] The U.S. government is also watching the trend and realizes that "[m]obile payment services and mobile wallets are changing the way consumers make retail payments, . . . offer[ing] the prospect of a banking relationship that exists only on a smartphone, tablet, or personal computer."[34]

These rapid and complex industry changes will continue for the foreseeable future, as will the scope and complexity of the nation's national security threats. Criminals, terrorists, and rogue states will surely adapt, and as they do, "new counter-measures must . . . [be] developed."[35] While responsive new countermeasures must be available to achieve the country's national security goals, governments and regulators need to coexist with industry so that innovation continues and for industry to answer market demands. Thus, sanctions and AML compliance will require new compliance paradigms and collaboration and information sharing between regulators and industry; because as the payments industry grows, and transaction speed and efficiency continue to increase, government regulators and private participants alike will have limited resources to tackle the growing compliance and oversight challenges. ■

[32] *Id.* at p. 4.

[33] *Fundamentals of Payment Systems*, *supra* note 6 at p. 18.

[34] *Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective*, *supra* note 9 at p. 3.

[35] *The Changing Face of the Payments System: A Policymaker's Guide to Important Issues*, *supra* note 4 at p. 8.