View on our website.

GIBSON DUNN

Anti-Money Laundering Update January 14, 2025

Top Year-End Developments in Anti-Money Laundering in 2024

Below we analyze the important trends and developments in Anti-Money Laundering (AML) regulation and enforcement by recapping significant developments during the last half of 2024.

This update includes a critical judicial decision striking down the Corporate Transparency Act; notable enforcement actions and prosecutions; key regulatory developments; and significant judicial opinions. We conclude with some thoughts about how a second Trump term likely will continue to bring significant AML enforcement actions and regulations.

1. Constitutional Challenges to the Corporate Transparency Act

The Corporate Transparency Act (CTA) was enacted in 2021, and (but for judicial developments described below) would require corporations, limited liability companies, and certain other entities created (or, as to non-U.S. entities, registered to do business) in any U.S. state or tribal jurisdiction to file a beneficial ownership interest (BOI) report with the U.S. Financial Crimes Enforcement Network (FinCEN) identifying, among other information, the natural persons who are beneficial owners of the entity.[1] A regulation, the Reporting Rule, helps implement the CTA by specifying compliance deadlines—including, at the time, a January 1, 2025 deadline for companies created or registered to do business in the United States before January 1, 2024—and detailing what information must be reported to FinCEN.[2]

In December 2024, a judge of the U.S. District Court for the Eastern District of Texas granted six plaintiffs' motion for a preliminary injunction.[3] The court held that the CTA exceeds Congress's

enumerated powers. In a 79-page opinion, Judge Amos L. Mazzant ruled that it was likely that the plaintiffs would be able to prove that:

- the CTA is not a proper exercise of Commerce Clause power because it does not regulate a channel or instrumentality of interstate commerce or any activity that substantially affects commerce[4]; and
- The CTA cannot be justified under the Necessary and Proper Clause because, contrary to the government's assertions, it is not rationally related to any enumerated power to regulate commerce, conduct foreign affairs, or collect taxes.[5]

The court's reasoning about the scope of the Commerce Clause, Necessary and Proper Clause, foreign affairs power, and taxing power echoed that of an earlier decision in the Northern District of Alabama.[6] While a judge of the U.S. District Court for the Northern District of Alabama had earlier enjoined enforcement of the CTA against only the plaintiffs in that case, the Eastern District of Texas went further. Observing that an injunction pertaining to plaintiff NFIB's approximately 300,000 members would be tantamount to a nationwide injunction, the court concluded that it was appropriate to preliminarily enjoin enforcement of the CTA and the Reporting Rule nationwide.[7] Moreover, the court invoked its power under the Administrative Procedure Act's stay provision, 5 U.S.C. § 705, to "postpone the effective date of" the Reporting Rule.[8]

Since the court's opinion, there has been a flurry of appeals and additional litigation. As of today, the CTA is unenforceable, enjoined by the U.S. Court of Appeals for the Fifth Circuit pending oral argument in March 2025.[9] The Department of Justice is currently appealing this ruling to the U.S. Supreme Court. Gibson Dunn has set up a Resource Center to provide a consolidated page with all of its client alerts about the current status of enforcement of the CTA, and additional updates will be posted there. Entities that believe they may be subject to the CTA and its associated Reporting Rule should closely monitor this matter, and consult with their CTA advisors as necessary, to understand their obligations and options. It is possible that the district court's injunction will again be stayed—and the CTA will become enforceable—on short notice.

Besides the Texas and Alabama decisions, three other federal courts also have ruled on the constitutionality of the CTA. Two courts upheld the statute.[10] Both sets of unsuccessful plaintiffs have appealed those rulings to the respective courts of appeal.[11] Another judge of the Eastern District of Texas recently held the statute unconstitutional.[12]

2. Enforcement Actions

There were a substantial number of enforcement actions brought in the latter months of 2024. Those include actions brought by DOJ, FinCEN, and state and federal bank regulators. Some of the most notable actions are discussed below.

a. AML and Money Laundering Resolutions involving T.D. Bank

On October 10, 2024, the Department of Justice, FinCEN, the Office of the Comptroller of the Currency (OCC), and the Board of Governors of the Federal Reserve Board (FRB), announced

landmark resolutions with T.D. Bank, N.A. (TDBNA) and its parent company TD Bank U.S. Holding Company (TDBUSH).

In the criminal resolutions, TDBUSH pled guilty to violating the Bank Secrecy Act by failing to maintain an adequate anti-money laundering (AML) program and failing to file accurate currency transaction reports (CTRs)[13]; and TDBNA pled guilty to conspiracy to violate the Bank Secrecy Act by failing to maintain an adequate AML program, failing to file accurate CTRs, and to launder money.[14] TDBNA agreed to forfeit more than $450 million, and TDBUSH agreed to a criminal fine of more than $1.4 billion, for a total financial criminal penalty of more than $1.8 billion. DOJ also imposed an independent monitor on TDBNA.

In the civil resolutions, FinCEN assessed a $1.3 billion civil monetary penalty on TDBNA and its affiliate T.D. Bank USA, N.A. for alleged willful violations of the BSA by failing to maintain an adequate AML program, and by allegedly willfully failing to file accurate and timely suspicious activity reports (SARs) and CTRs.[15] FinCEN also imposed an independent monitorship. The OCC assessed a $450 million civil monetary penalty on TDBNA and T.D. Bank USA, N.A. for failing to develop and maintain an adequate AML program.[16] The OCC imposed restrictions on growth at TDBNA and T.D. Bank USA, N.A. The FRB assessed a civil monetary penalty of more than $123 million on TDBUSH and the other T.D. Bank parent companies.[17] In total, given various credit and off-sets between the authorities, T.D. Bank affiliated entities agreed to pay more than $3.1 billion in financial penalties, one of the largest financial penalties ever paid by a financial institution.

These resolutions are notable for several reasons. First, the actions show authorities' interest in pursuing charges that financial institutions allegedly willfully violated the BSA based on the purported high costs of compliance. Second, the resolutions indicate that the government may second-guess compliance resourcing decisions. Third, DOJ criminally prosecuted TDBNA for the relatively novel charge of money laundering on this fact pattern, beyond the more standard charges of violating the BSA. A money laundering conviction for a financial institution can trigger license revocation proceedings. Finally, DOJ and FinCEN each imposed monitorships, and each agency reserves the sole discretion to select a monitor, meaning that there is a chance that two different monitors with overlapping remits will be appointed and report to different agencies.

b. Stepped Up Enforcement Involving Casinos

On September 6, 2024, Wynn Las Vegas (WLV) entered into a Non-Prosecution Agreement alleging that Wynn "illegally used unregistered money transmitting businesses to circumvent the conventional financial system."[18] According to DOJ, WLV contracted with third-party independent agents that transferred foreign gamblers' funds through "companies, bank accounts, and other third-party nominees in Latin America and elsewhere, and ultimately into a WLV-controlled bank account."[19] The money was then transferred into a WLV cage account, which employees credited to the WLV account of each individual patron, enabling these gamblers to allegedly "evade foreign and U.S. laws governing monetary transfer and reporting."[20] In other instances, WLV allegedly knowingly failed to report suspicious activity or scrutinize the source of funds.[21] WLV agreed to forfeit $130,131,645 to settle the allegations against it.[22]

On October 22, 2024, FinCEN imposed a $900,000 civil money penalty on Sahara Dunes Casino, LP (d/b/a Lake Elsinore Hotel and Casino) for implementing an allegedly "fundamentally unsound" AML program, violating the BSA and its implementing regulations.[23] As part of its settlement with FinCEN, the California gaming establishment admitted to willfully failing to implement and maintain a written AML program that met minimum BSA requirements, file timely CTRs, make accurately and timely reports of suspicious transactions, and maintain records consistent with the BSA.[24] For example, FinCEN alleged that it had identified more than ten instances in 2017 alone where Sahara Dunes was required to file a CTR but failed to do so in a timely fashion; and alleged dozens of instances in which the casino failed to file a SAR or filed the SAR late. Sahara Dunes agreed to hire a qualified independent consultant to review the casino's AML program.[25]

These actions, and the DOJ's criminal charges against a casino executive and non-prosecution agreements with two casinos earlier in 2024,[26] are indicative of authorities' ongoing interest in AML programs at casinos and other gambling entities.

c. Novel Money Laundering and Forfeiture Theory Involving McKinsey

On December 13, 2024, the DOJ entered into a series of resolutions with McKinsey & Company Inc.[27] The resolutions involved McKinsey's consulting work for Purdue Pharma L.P., relating to McKinsey's advice concerning OxyContin. McKinsey entered into a deferred prosecution agreement, entered into a settlement of a forfeiture action brought by DOJ, and also settled claims brought under the civil False Claims Act. In sum, McKinsey agreed to pay $650 million to resolve the claims. The resolution included the novel assertion by DOJ that because McKinsey received approximately $7 million of alleged proceeds of narcotics trafficking from Purdue in 2013 and 2014, which McKinsey commingled with its other legitimate monies, McKinsey itself was property involved in money laundering and thus forfeitable to the government under the federal civil forfeiture laws.[28] McKinsey and the DOJ agreed to settle the forfeiture complaint for just over $93 million, which DOJ alleged is the amount of money Purdue paid to McKinsey "[o]ver the course of 75 engagements from 2004 through 2019."[29]

d. Other Bank Actions

On September 12, 2024, the OCC entered into an agreement with Wells Fargo Bank, N.A, after the OCC identified alleged deficiencies relating to Wells Fargo's AML internal controls.[30] As part of the agreement, Wells Fargo agreed to create a compliance committee charged with implementing the Agreement and monitoring and overseeing the Bank's compliance with the Agreement in general.[31] The Agreement does not impose a financial penalty.

On August 27, 2024, the New York Department of Financial Services (DFS) imposed a $35 million penalty on Nordea Bank Abp for allegedly significant compliance failures with respect to AML requirements, and the bank's failure to conduct proper due diligence of its correspondent bank partners.[32] DFS investigated Nordea after the 2016 Panama Papers leak exposed Nordea's alleged role in helping customers create offshore tax-sheltered companies and entities connected to money laundering operations.[33] DFS found that Nordea failed to maintain an effective and compliant AML program, failed to conduct adequate due diligence in its

correspondent bank relationships, and failed to maintain an adequate transaction monitoring system.[34]

e. FinCEN Finding Against Russian Virtual Currency Exchanger

On September 26, 2024, FinCEN took further steps to disrupt alleged Russian cybercrime services. Specifically, FinCEN issued an order that identified PM2BTC—a Russian virtual currency exchanger—as a "primary money laundering concern."[35] According to FinCEN, through PM2BTC's currency exchange activities, monies passing through the exchange relate to fraud schemes, sanctions evasion efforts, ransomware attacks, and instances of child abuse.[36] The order effectively prohibits U.S. financial institutions from engaging in financial transactions with PM2BTC.[37] The order comes on the heels of increased enforcement steps taken pursuant to the Combatting Russian Money Laundering Act; this is the second order issued pursuant to that statute.[38]

f. Notable Sentencings

The last few months of 2024 also brought notable sentencings in long-running cryptocurrency money laundering cases.

On November 8, 2024, Roman Sterlingov was sentenced to twelve years and six months' imprisonment for his operation of a bitcoin money laundering service.[39] Sterling was convicted at trial earlier in 2024 on counts of conspiracy to commit money laundering and operating an unlicensed money transmitting business, for running a service called "Bitcoin Fog." According to the government, Bitcoin Fog was a darknet site that made it more difficult to trace crypto transactions on public blockchains to identifiable entities and persons. The site was allegedly used to launder the proceeds of various criminal conduct, including narcotics trafficking and child sexual abuse material.

On November 14, 2024, Ilya Lichtenstein was sentenced to five years in prison for his 2016 hack of cryptocurrency exchange Bitfinex, and his subsequent conspiracy to launder hundreds of thousands of Bitcoin stolen in the hack.[40] In 2016, Lichtenstein hacked into Bitfinex's network and fraudulently authorized over 2,000 transactions transferring 119,754 Bitcoin to his cryptocurrency wallet. Lichtenstein then deleted network access credentials and log files connected to him and, with the help of his wife Heather "Razzlekhan" Morgan,[41] laundered the funds through various fictitious identities, darknet markets, and cryptocurrency exchanges. Lichtenstein received credit for cooperating with authorities, including by testifying at Sterlingov's trial.

On November 15, 2024, after years of litigation, Larry Dean Harmon was sentenced to three years' imprisonment for operating Helix, a popular darknet cryptocurrency mixer.[42] Harmon previously pled guilty to conspiracy to commit money laundering. Harmon also received credit for cooperating with authorities, and also testified at Sterlingov's trial.

3. Regulatory Developments and Guidance

a. Final Investment Adviser and Real Estate AML Rules

Early in 2024, FinCEN issued proposed rules extending certain AML requirements to residential real estate transactions, and to registered investment advisers. On August 28, 2024, FinCEN released the final rules for both.[43]

The final investment advisers rule (the "Investment Advisers Rule")[44] will take effect January 1, 2026. The Investment Advisers Rule adds certain investment advisers to the definition of "financial institutions" governed by the BSA. The Investment Advisers Rule covers advisers who are registered or required to register with the Securities and Exchange Commission (SEC), with a few narrow exceptions, and those that report to the SEC as Exempt Reporting Advisers.[45] For investment advisers based outside of the United States, the Investment Advisers Rule only applies to advisory activities that (i) take place within the United States, including through the involvement of U.S. personnel or (ii) provide advisory services to a U.S. person or a foreign-located private fund with an investor that is a U.S. person.[46]

Under the Investment Advisers Rule, covered investment advisers will be required to, among other things, implement risk-based AML programs, file SARs with FinCEN, and keep records relating to the transmittal of funds that equal or exceed $3,000.[47] The Investment Advisers Rule also applies information-sharing provisions between and among FinCEN, law enforcement government agencies, and certain financial institutions.[48] FinCEN delegated examination/supervisory authority to the SEC, given the SEC's expertise in supervising the investment adviser industry.[49]

The final real estate rule (the "Real Estate Rule")[50] will take effect December 1, 2025. The Real Estate Rule covers non-financed transfers of various types of residential real estate, including single-family houses, townhouses, condominiums, cooperatives, and other buildings designed for occupancy by one to four families.[51] A transaction is considered "non-financed" if it does not involve an extension of credit issued by a financial institution required to maintain an AML program and file SARs.[52] There are exemptions from the Real Estate Rule for some common, low-risk types of transfers such as transfers resulting from death, divorce, or to a bankruptcy estate.[53]

The Real Estate Rule identifies persons required to file a report ("Reporting Person(s)") through a "cascade" framework which assigns the reporting responsibility in sequential order to various persons who perform closing or settlement functions for residential real estate transfers.[54] The cascade is as follows: (1) the person listed as the closing agent; (2) the person who prepares the closing statement; (3) the person who files the transfer document (e.g., deed) with the recordation office; (4) the person who underwrites an owner's title insurance policy for the transferee; (5) the person who disburses the greatest amount of funds in connection with the transfer; (6) the person who provides an evaluation of the status of the title; and (7) the person who prepares the deed or similar legal instrument.[55] Alternatively, persons specified in this list can designate by written agreement who will serve as a Reporting Person for the transfer.[56]

b. Proposed AML Program Rule

In the Anti-Money Laundering Act of 2020 (AMLA), Congress mandated the "[e]stablishment of national exam and supervision priorities."[57] The AMLA made a number of changes to the Bank Secrecy Act, including that compliance programs remain "risk-based," and requiring that the Secretary of the Treasury "establish and make public priorities for anti-money laundering."

In 2021, the government published its AML/CFT priorities, which include "corruption, cybercrime, domestic and international terrorist financing, fraud, transnational criminal organizations, drug trafficking organizations, human trafficking and human smuggling, and proliferation financing."[58] SAR filings are now required to be guided in part by "the risk assessment processes of the covered institution," with consideration for the government's priorities The purpose of the amendments in the AMLA was to "strengthen, modernize, and improve" FinCEN's ability to communicate, oversee, and process its AML and CFT program.

In July 2024, FinCEN issued a notice of proposed rulemaking on Anti-Money Laundering and Countering the Financing of Terrorism Programs (the "AML Program Rule").[59] The AML Program Rule was designed to ensure that financial institutions "implement[] an effective, risk-based, and reasonably designed AML/CFT program to identify, manage, and mitigate illicit finance activity risks." The proposed rule includes a mandatory risk assessment process. The proposed rule also would require financial institutions to review government-wide AML/CFT priorities and incorporate them, as appropriate, into risk-based programs. The proposed rule also articulated certain broader considerations for an effective and risk-based AML/CFT framework as envisioned by the AMLA.

c. Guidance to Prosecutors Regarding Corporate Compliance Programs

On September 23, 2024, the DOJ Criminal Division announced the latest revision of its Evaluation of Corporate Compliance Programs (the ECCP).[60] The ECCP serves as the Criminal Division's guidance for its prosecutors to evaluate companies' compliance programs when making enforcement decisions. This revision focused on how organizations proactively identify, mitigate, and manage the risks associated with their use of emerging technologies, including AI. This emphasis reflects DOJ's increasing focus on companies' use of data and technology and its expectations that companies' approach to risk management will be proactive rather than reactive. The ECCP recognized that AI will affect AML programs. The general guidance provided to entities includes:

- Documenting the entity's use of AI and other new technologies and plan out steps for identifying the risk level for intended uses (e.g., in circumstances where the particular use of AI creates particular risks, such as confidentiality, privacy, cybersecurity, quality control, bias, etc.);

- Deploying a sufficient degree of human oversight, especially for high-risk uses, and whether the performance of those systems is being assessed by reference to an appropriate "baseline of human decision-making" (e.g., the expected standard to which human decision-makers would be held for a given use case);

- Monitoring and testing their technology to evaluate if it is functioning "as intended," both in their commercial business and compliance program, and consistent with the laws and the company's code of conduct.

4. Key Judicial Decisions

The last few months also featured important judicial decisions regarding the anti-money laundering and sanctions laws, both involving the decentralized cryptocurrency platform Tornado Cash. Tornado Cash is an open-source software protocol that facilitates private digital asset transactions, originally developed by a team of developers allegedly including Roman Storm, Alexey Pertsev and Roman Semenov.

a. Fifth Circuit OFAC Decision

On November 26, 2024, a unanimous panel of the Fifth Circuit Court of Appeals ruled in favor of users of Tornado Cash, striking down the Office of Foreign Asset Control's (OFAC) attempt to add certain property of Tornado Cash to the Specially Designated Nationals (SDN) List.[61] In 2019, the developers uploaded the Tornado Cash protocol to the Ethereum blockchain via a series of open-source computer code known as "smart contracts". In late 2022, OFAC added Tornado Cash to the SDN List and designated the smart contracts underlying the Tornado Cash protocol as blocked "property." In doing so, OFAC alleged that Tornado Cash had been used by North Korean entities to commit cybercrimes including the laundering of stolen cryptocurrency.[62] Six users of Tornado Cash brought suit challenging OFAC's determination, arguing that the addition of Tornado Cash to the SDN list was outside of OFAC's authority under the International Emergency Economic Powers Act ("IEEPA") and the North Korea Sanctions and Policy Enhancement Act.[63] The district court disagreed and dismissed the suit.[64]

The Fifth Circuit reversed. The Fifth Circuit first concluded that the plain text of the applicable statutes, which authorizes the government to block only "property," does not encompass immutable smart contracts because they are incapable of being owned.[65] The Fifth Circuit further concluded that the smart contracts do not qualify as "property" even under OFAC's regulatory definition of "property," which includes "contracts" and "services." The court determined that these "smart contracts" are not legal "contracts" at all.[66] Rather, they are "nothing more than lines of code."[67] Finally, the court held that the smart contracts are not "services," but instead "*tools* used in providing a service," which is "not the same as *being* a service."[68] In short, "the immutable smart contracts are not property because they are not ownable, not contracts, and not services."[69] As a result, the Fifth Circuit concluded that OFAC lacks authority to add the Tornado Cash smart contracts to the SDN List.[70]

b. Southern District of New York MSB Decision

In a September 27, 2024 oral ruling, Judge Katherine Polk Failla of the Southern District of New York denied a motion to dismiss charges against Tornado Cash developer Roman Storm.[71] In 2023, Storm was charged with conspiracy to commit money laundering, conspiracy to operate an unlicensed money transmitting business, and conspiracy to violate U.S. sanctions.[72] Storm moved to dismiss the charges, asserting (among other things) that his conduct, as charged in the Indictment, lies outside the scope of each applicable criminal statute.[73]

Judge Failla denied Storm's motion to dismiss on statutory grounds. With respect to the unlicensed money transmitting charge, she held that the law applied to entities that do not maintain control over the funds being accepted or transmitted;[74] and held that the Indictment had adequately alleged that Tornado Cash charged fees for its services.[75] With respect to the money laundering charge, Judge Failla held that because the Indictment adequately alleged that Tornado Cash was a money transmitting business, transactions with the entity constituted "financial transactions" under the money laundering laws.[76] Finally, the court denied the motion to dismiss with respect to conspiracy to violate U.S. sanctions, rejecting Storm's argument that Tornado Cash's software was merely "informational materials," subject to an exception to the law.[77] Judge Failla also rejected the defendant's constitutional challenges to the Indictment.[78] Notably, citing the Fifth Circuit's decision, the defendant recently moved the Court to reconsider its decisions; that motion is pending.[79]

5. Incoming Administration

Overall, we expect that anti-money laundering enforcement will remain a key area of focus under the second Trump Administration, though we also expect some shift in specific priorities. As a general matter, combatting money laundering has generally been a bipartisan issue. During the first Trump Administration, there were important regulatory and enforcement actions related to the anti-money laundering laws.[80] Indeed, high-ranking regulators at FinCEN and OCC at a November 2024 conference stated they expect continued focus on AML enforcement through the new Administration.[81]

During his campaign, President-Elect Trump also made policy announcements consistent with continued enforcement of the BSA, for example promising to "cut off [drug] cartels' access to the global financial system" and "get full cooperation of neighboring governments to dismantle the cartels, or else fully expose the bribes and corruption that protect these criminal networks."[82] His campaign also focused on continued pressure on North Korea and Iran, which implicitly puts focus on financial institutions' AML and sanctions programs.

That said, it is possible that the new Administration may cut back on some of the more novel enforcement and regulatory actions brought during the Biden Administration. For instance, some members of President Elect Trump's Administration have opposed the Corporate Transparency Act.[83] A second Trump Administration may also deemphasize enforcement actions targeting the cryptocurrency industry, which has been a major focus of the Biden Administration.

It is possible that some of the Department of Treasury's existing priorities will also change. For example, there may be fewer FinCEN alerts on certain topics, including, for example, environmental crimes or wildlife trafficking that received more emphasis during the Biden Administration.

Using the Congressional Review Act, Congressional Republicans and the Administration may seek to strike down the Registered Investment Adviser and Real Estate regulations, and may also revise the AML Program rule.[84]

Conclusion

2024 was a notable year in the AML enforcement space. We anticipate that 2025 will be similarly active, as litigation challenging the CTA continues to unfold, and the incoming Trump Administration looks to AML enforcement as a way to advance its own policy priorities involving illegal immigration and narcotics trafficking. We will continue to monitor these updates and report accordingly on steps individuals and entities should take to navigate the ever-changing regulatory regime.

Please click on the link below to view the complete update and endnotes on Gibson Dunn's website:

Read More

The following Gibson Dunn lawyers assisted in preparing this update: Stephanie Brooker, M. Kendall Day, Ella Capone, Sam Raymond, Maura Carey, Rachel Jackson, Ben Schlichting, Karsyn Archambeau*, and Aquila Maliyekkal*.

Gibson Dunn has deep experience with issues relating to the Bank Secrecy Act, other AML and sanctions laws and regulations, and the defense of financial institutions more broadly. For assistance navigating white collar or regulatory enforcement issues involving financial institutions, please contact any of the authors, the Gibson Dunn lawyer with whom you usually work, or any of the leaders and members of the firm's Anti-Money Laundering / Financial Institutions, Financial Regulatory, White Collar Defense & Investigations, or International Trade practice groups:

Anti-Money Laundering / Financial Institutions:
Stephanie Brooker – Washington, D.C. (+1 202.887.3502, sbrooker@gibsondunn.com)
M. Kendall Day – Washington, D.C. (+1 202.955.8220, kday@gibsondunn.com)
Ella Alves Capone – Washington, D.C. (+1 202.887.3511, ecapone@gibsondunn.com)

White Collar Defense and Investigations:
Stephanie Brooker – Washington, D.C. (+1 202.887.3502, sbrooker@gibsondunn.com)
Winston Y. Chan – San Francisco (+1 415.393.8362, wchan@gibsondunn.com)
Nicola T. Hanna – Los Angeles (+1 213.229.7269, nhanna@gibsondunn.com)
F. Joseph Warin – Washington, D.C. (+1 202.887.3609, fwarin@gibsondunn.com)

Global Fintech and Digital Assets:
M. Kendall Day – Washington, D.C. (+1 202.955.8220, kday@gibsondunn.com)
Jeffrey L. Steiner – Washington, D.C. (+1 202.887.3632, jsteiner@gibsondunn.com)
Sara K. Weed – Washington, D.C. (+1 202.955.8507, sweed@gibsondunn.com)

Global Financial Regulatory:
William R. Hallatt – Hong Kong (+852 2214 3836, whallatt@gibsondunn.com)

Michelle M. Kirschner – London (:+44 20 7071 4212, mkirschner@gibsondunn.com)
Jeffrey L. Steiner – Washington, D.C. (+1 202.887.3632, jsteiner@gibsondunn.com)

International Trade:
Ronald Kirk – Dallas (+1 214.698.3295, rkirk@gibsondunn.com)
Adam M. Smith – Washington, D.C. (+1 202.887.3547, asmith@gibsondunn.com)

Karsyn Archambeau and Aquila Maliyekkal, associates in New York and Washington, D.C. respectively, are not yet admitted to practice law.