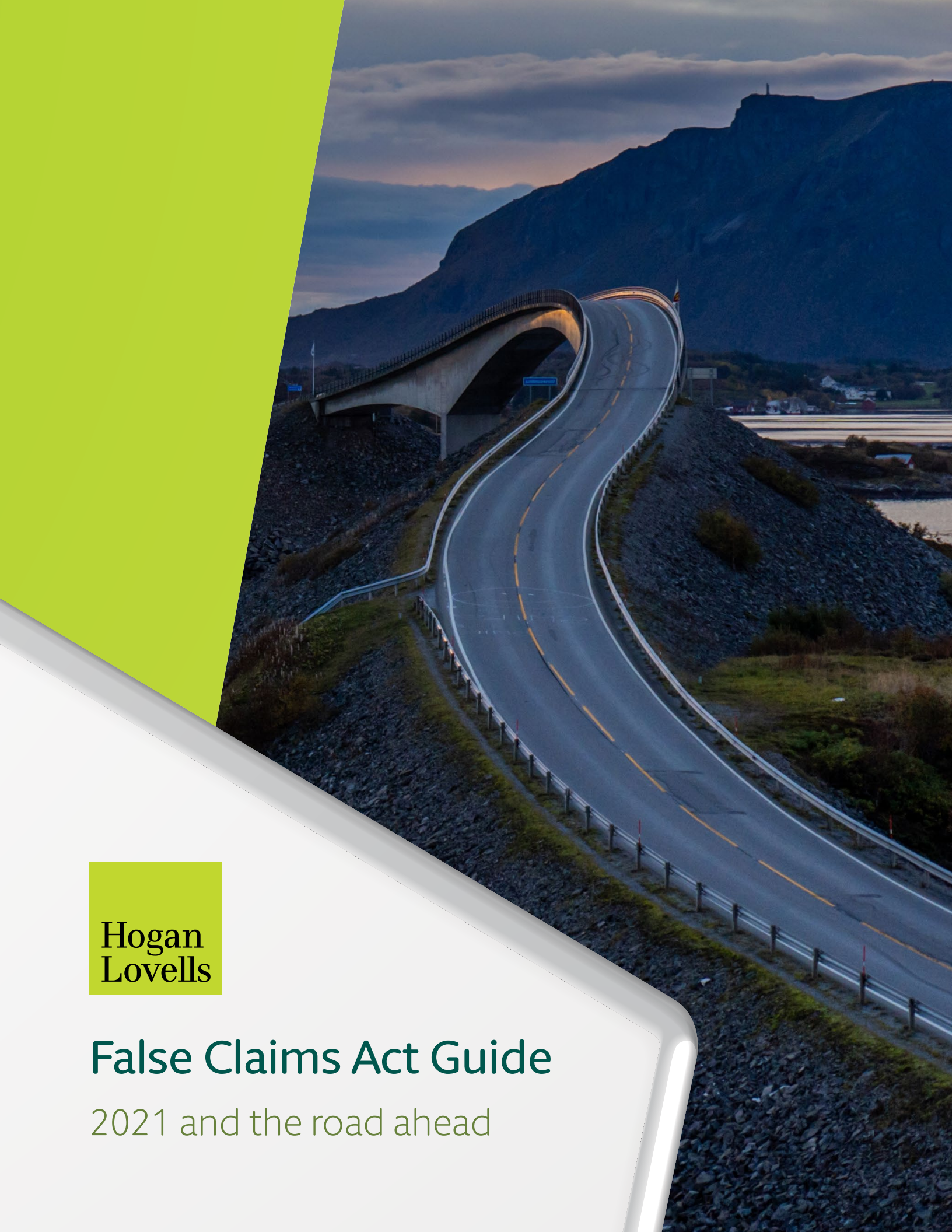
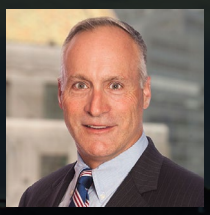


Hogan Lovells

False Claims Act Guide

2021 and the road ahead

Editors



Anthony E. Fuller
Partner | Boston
+1 617 371 1032
anthony.fuller@hoganlovells.com

Gejaa Gobena
Partner | Washington, D.C.
+1 202 637 5513
gejaa.gobena@hoganlovells.com

Michele Sartori
Partner | Washington, D.C.
+1 202 637 6443
michele.sartori@hoganlovells.com

David I. Sharfstein
Partner | Washington, D.C., Baltimore
+1 202 637 5739 (Washington, D.C.)
+1 410 659 2721 (Baltimore)
david.sharfstein@hoganlovells.com

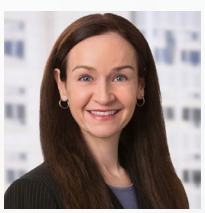
2021 and the road ahead

Executive summary

2021 ushered in a new administration, new U.S. Department of Justice (DOJ) officials, and, of course, new DOJ policies and initiatives – many of which implicate the False Claims Act (FCA). But one thing that remained constant was DOJ's use of the FCA as a key enforcement tool.

While DOJ renewed its focus on telehealth and cyber-fraud, the courts continued to develop jurisprudence, and sometimes confusion, in the FCA arena. Meanwhile, potentially significant amendments to the FCA are being considered in the Senate, which may impact materiality and government dismissals. We hope this guide provides a useful review of the most noteworthy FCA developments – both on the DOJ enforcement front and the developing case law and legislative landscape – and a preview of potential FCA developments to come in 2022.

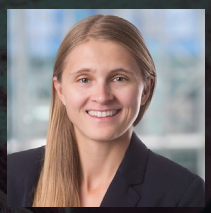
Gejaa Gobena
Partner | Washington, D.C.
+1 202 637 5513
gejaa.gobena@hoganlovells.com



Michele Sartori
Partner | Washington, D.C.
+1 202 637 6443
michele.sartori@hoganlovells.com

Michele Sartori
Partner | Washington, D.C.
+1 202 637 6443
michele.sartori@hoganlovells.com

Allison Caplis
Counsel | Baltimore
+1 410 659 2784
allison.caplis@hoganlovells.com



Hunter Davis
Associate | Washington, D.C.
+1 202 804 7892
hunter.davis@hoganlovells.com

Healthcare digitization creates new FCA risk

In recent years, the implementation of electronic health records (EHR) and rapid expansion of telemedicine has caught the attention of the Department of Justice (DOJ) and the qui tam relators' bar, prompting rigorous enforcement actions and increasing False Claims Act (FCA) cases. Despite shifts in technology reshaping patient records and care, FCA enforcement remains a constant and growing force.

Telemedicine fraud had attracted DOJ attention before the pandemic

DOJ has traditionally been wary of telemedicine. Even before the COVID-19 pandemic and the accompanying rapid expansion of telehealth, enforcement in the telemedicine industry was on the rise. In 2019, DOJ pursued enforcement actions in the telehealth space that involved claims for durable medical equipment (DME) and for compound medicines.

Through "Operation Brace Yourself," DOJ targeted an alleged fraud and kickback scheme through which DME companies paid illegal kickbacks and bribes to medical professionals working for fraudulent telemedicine companies. In exchange, the medical professionals referred Medicare beneficiaries to the conspiring DME companies for back, shoulder, wrist, and knee braces that were medically unnecessary. The DOJ investigation resulted in enforcement actions against 24 defendants associated with five telemedicine companies, as well as the owners of dozens of durable medical equipment companies and three licensed medical professionals.[1] According to DOJ, the fraud schemes involved more than $1.2 billion in loss.[2]

Also in 2019, a physician agreed to pay $300,000 to resolve allegations that he violated the FCA by causing "pharmacies to submit false claims for compounded medications to TRICARE by issuing or approving prescriptions which were invalid, because [the physician] did not speak with or examine the patients in question and did not have an established physician-patient relationship with them. . ." [3]

Pandemic-era telemedicine boom increases opportunities for fraud and abuse

Traditionally, Medicare's coverage of telemedicine has been extremely limited. As a result of the pandemic, telehealth service providers were granted broad flexibility to provide telemedicine services and this flexibility remains today. The easing of

1. Press Release, U.S. Dep't of Justice, Federal Indictments & Law Enforcement Actions in One of the Largest Health Care Fraud Schemes Involving Telemedicine and Durable Medical Equipment Marketing Executives Results in Charges Against 24 Individuals Responsible for Over $1.2 Billion in Losses (April 9, 2019), https://www.justice.gov/opa/pr/federal-indictments-and-law-enforcement-actions-one-largest-health-care-fraud-schemes.
2. *Id.*
3. Press Release, U.S. Dep't of Justice, Federal Health Care Fraud Takedown in Northeastern U.S. Results in Charges Against 48 Individuals (Sept. 26, 2019), https://www.justice.gov/opa/pr/federal-health-care-fraud-takedown-northeastern-us-results-charges-against-48-individuals.

restrictions stemming from the COVID-19 pandemic has prompted a dramatic increase in the use of telehealth.[4] It seems unlikely that the federal government will reinstate pre-pandemic restrictions on telehealth services given the increased popularity and reliance on telehealth services. Indeed, Congress has introduced several bipartisan bills to address post-pandemic telehealth services, signaling that utilization of telehealth services will likely remain prevalent.[5]

While regulatory flexibility for telehealth services has expanded health care access and improved health care services, it has also increased opportunities for fraud and abuse. And the government has demonstrated a resolve to stamp out fraud and corruption in the telemedicine industry, including through use of the FCA.

In October of 2020, DOJ announced a telehealth enforcement action for a fraudulent DME billings scheme dubbed "Operation Rubber Stamp." The scheme involved defendant telemedicine executives allegedly paying medical professionals to order DME, genetic and other diagnostic testing, and pain medications without sufficient patient diagnostic interaction, resulting in $1.5 billion in fraudulent billings to government health care insurance programs.[6] To date, this investigation has led to criminal charges of health care fraud, false statements, violations of the federal Anti-Kickback Statute (AKS) and related conspiracies against more than 30 individuals. Although DOJ has not announced any related FCA actions yet, such fraud schemes could eventually prompt FCA claims by DOJ or whistleblowers.

In contrast, FCA violations *have been* alleged and resolved in an ongoing investigation dubbed operation "Happy Clickers," which involves allegations that physicians "approved orders for medically unnecessary braces and cancer genetic testing despite many red flags that these items and services were illegitimate."[7]

The transition to electronic health records has also created FCA risk

Electronic health records are computerized versions of a patient's medical history maintained by his or her health care provider over time, which have automated access to patient information and offer the potential to streamline patient care while improving the accuracy and clarity of medical records.[8]

4. According to a Department of Health and Human Services report published in July 2020, less than one percent (0.1%) of Medicare visits were provided through telehealth before the COVID-19 Public Health Emergency, while in April 2020, almost half (43.5%) of Medicare primary care visits were provided through telehealth. *Medicare Beneficiary Use of Telehealth Visits: Early Data from the Start of the Covid-19 Pandemic*, Assistant Sec'y for Planning and Evaluation, U.S. Dep't of Health and Human Servs. (July 28, 2020), https://aspe.hhs.gov/sites/default/files/private/pdf/263866/hp-issue-brief-medicare-telehealth.pdf.

5. *See, e.g.*, TELE HEALTH HSA Act of 2021, 117th Cong. (1st Sess. 2021), https://www.congress.gov/bill/117th-congress/senate-bill/2097?s=1&r=58; and the Advancing Telehealth Beyond COVID-19 Act of 2021, 117th Cong. (1st Sess. 2021), https://www.congress.gov/bill/117th-congress/house-bill/4040/text?r=9.

6. Press Release, U.S. Dep't of Justice Operation Rubber Stamp: Major health care fraud investigation results in significant new charges (Oct. 7, 2020), https://www.justice.gov/usao-sdga/pr/operation-rubber-stamp-major-health-care-fraud-investigation-results-significant-new.

7. Press Release, U.S. Dep't of Justice, U.S. Attorney Announces Criminal and Civil Enforcement Actions Against Medical Practitioners For Roles in Telemedicine Fraud Schemes, U.S. Dep't of Justice (Aug. 24, 2021), https://www.justice.gov/usao-wdmi/pr/2021_0824_Happy_Clickers.

8. *Electronic Health Records*, Centers for Medicare & Medicaid Services, CMS.gov, https://www.cms.gov/Medicare/E-Health/EHealthRecords (last modified on Mar. 26, 2012, 11:42 AM).

In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health Act (HITECH Act) establishing the Medicare and Medicaid Electronic Health Records Incentive Programs.[9] The statute provided over $30 billion for incentive payments to physicians and hospitals to encourage them to transition to EHR and make "meaningful use" (MU) of the software.[10] In order to obtain these incentives and, at present avoid penalties,[11] health care providers must warrant that they satisfied certain Department of Health and Human Services (HHS)-adopted criteria, including utilizing approved EHR software and achieving various utilization milestones. The EHR software companies are required to provide software that meets specific MU standards around the functionality of the software. In order to demonstrate that the EHR software could meet the MU standards, the software was required to pass tests performed by an independent, accredited testing laboratory, followed by certification from an independent, accredited certification body authorized by HHS.[12]

In recent years, DOJ has pursued several FCA cases related to EHR that have led to large settlements and highlight various FCA risks for EHR companies and those doing business with them.

- Discounts in exchange for referrals. In January of 2019, Inform Diagnostics, a pathology laboratory company, paid $63.5 million to resolve FCA allegations arising from claims that the company violated the AKS and the Stark Law "by engaging in improper financial relationships with referring physicians" by subsidizing their EHR systems and providing them discounted technology consulting services in exchange for patient referrals for laboratory services.[13]
- Product capability misrepresentations. In February of 2019, Greenway Health LLC agreed to pay $57.25 million to resolve an FCA action alleging it caused its users to "submit false claims to the government by misrepresenting the capabilities of its EHR product 'Prime Suite' and providing unlawful remuneration to users to induce them to recommend Prime Suite."[14]
- Misrepresenting eligibility for EHR Incentives. In May of 2019, Coffrey Health System agreed to pay $250,000 to resolve FCA allegations that it submitted false claims to

9. H.R. 1, 111th Cong. (2009), https://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf.
10. *Id.*; *see also*, Adler-Milstein, Julia and Ashish K. Jha, *HITECH Act Drove Large Gains In Hospital Electronic Health Record Adoption*, HealthAffairs.org (Aug. 2017), https://www.healthaffairs.org/doi/10.1377/hlthaff.2016.1651.
11. The incentive payments of the HITECH act were in place until 2015. Since that time, health care providers who cannot demonstrate that they are utilizing approved EHR software are subject to certain penalties in the form of reduced Medicare reimbursements.
12. Press Release, U.S. Dep't of Justice, *Kansas Hospital Agrees to Pay $250,000 To Settle False Claims Act Allegations* (May 31, 2019), https://www.justice.gov/usao-ks/pr/kansas-hospital-agrees-pay-250000-settle-false-claims-act-allegations; Press Release, U.S. Dep't of Justice, Electronic Health Records Vendor to Pay $57.25 Million to Settle False Claims Act Allegations (Feb. 6, 2021), https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-5725-million-settle-false-claims-act-allegations.
13. Press Release, U.S. Dep't of Justice, Pathology Laboratory Agrees to Pay $63.5 Million for Providing Illegal Inducements to Referring Physicians (Jan. 30, 2019), https://www.justice.gov/opa/pr/pathology-laboratory-agrees-pay-635-million-providing-illegal-inducements-referring.
14. Press Release, U.S. Dep't of Justice, Electronic Health Records Vendor to Pay $57.25 Million to Settle False Claims Act Allegations (Feb. 6, 2021), https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-5725-million-settle-false-claims-act-allegations.

the Medicare and Medicaid Programs under the EHR Incentive Program by falsely attesting "that it conducted and/or reviewed security risk analyses" required by HHS.[15]

- Improper kickbacks in exchange for improper Clinical Decision Support programing. In 2020, Practice Fusion Inc. (Practice Fusion), a health information technology developer, paid $145 million to resolve criminal and civil investigations relating to its EHR software, including a $118.6 million FCA settlement.[16] The resolution addressed allegations that Practice Fusion "extracted unlawful kickbacks from pharmaceutical companies in exchange for implementing clinical decision support (CDS)[17] alerts in its EHR software designed to increase prescriptions for their drug products."[18] In particular, Practice Fusion allowed pharmaceutical companies to shape the creation and implementation of the CDS alerts in ways aimed at advancing the sales of the companies' products, and such alerts were not always a reflection of accepted medical standards.[19]
- Improper remuneration schemes. Finally, on January 28, 2021, DOJ announced a $18.25 million FCA and AKS settlement with athenahealth Inc. (Athena), resolving two separate qui tam lawsuits. The United States alleged that Athena violated the FCA and AKS by (1) inviting new and existing customers to "Concierge Events," including sporting events like the Masters Tournament and the Kentucky Derby with complimentary travel and luxury accommodations; (2) paying kickbacks to existing customers for each new client that signed up for Athena services; and (3) brokering deals with competing EHR vendors that were discontinuing their EHR services to refer their clients to Athena in exchange for remuneration based on the value and volume of their practices.[20]

15. Press Release, U.S. Dep't of Justice, Kansas Hospital Agrees to Pay $250,000 To Settle False Claims Act Allegations (May 31, 2019), https://www.justice.gov/usao-ks/pr/kansas-hospital-agrees-pay-250000-settle-false-claims-act-allegations.
16. Press Release, U.S. Dep't of Justice, Electronic Health Records Vendor to Pay $145 Million to Resolve Criminal and Civil Investigations (Jan. 27, 2020), https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0.
17. The Practice Fusion deferred prosecution agreement defines CDS to include "computerized alerts and reminders to care providers and patients; clinical guidelines; condition-specific order sets; focused patient data reports and summaries; documentation templates; diagnostic support, and contextually relevant reference information, among other tools."
18. *Id.*
19. *Id.*
20. Press Release, U.S. Dep't of Justice, Electronic Health Records Technology Vendor to Pay $18.25 Million to Resolve Kickback Allegations (Jan. 28, 2021), https://www.justice.gov/opa/pr/electronic-health-records-technology-vendor-pay-1825-million-resolve-kickback-allegations.

What's next?

We expect FCA and other fraud investigations relating to telehealth fraud and EHR to continue. Brian M. Boynton, Acting Assistant Attorney General for the Civil Division at the Department of Justice, recently stated that he expects "a continued focus on telehealth schemes, particularly given the expansion of telehealth during the pandemic."[21] He also identified fraud relating to EHR as another area that is likely to be a focal point of future enforcement efforts.[22]

The Department of Health and Human Services Office of Inspector General (OIG) has also made clear that it is "conducting significant oversight work assessing telehealth services during the public health emergency."[23]

In light of expanded government scrutiny and enforcement in the telehealth space, telemedicine companies and providers should evaluate their compliance programs. Providers should be aware of potential government scrutiny of the length of telemedicine visits, as well as DME and genetic testing prescriptions. Further, providers should ensure that physician-patient relationships and encounters are properly documented and monitor any proposed legislative and regulatory changes.[24]

In anticipation of continued government oversight and enforcement into EHR, EHR companies should confirm that their products are compliant with EHR incentive program requirements. EHR organizations should ensure that they maintain a robust compliance function around software development and implementation, keeping abreast of certification requirements and standards, training members of its workforce on these requirements, and conducting risk assessments to isolate and fix vulnerabilities. Meanwhile, health care providers should ensure their selected EHR software is properly certified by HHS and has previously maintained successful reliable outcomes.[25]

21. Press Release, U.S. Dep't of Justice, Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Federal Bar Association Qui Tam Conference (Feb. 17, 2021), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-federal-bar.

22. Press Release, U.S. Dep't of Justice, Acting Assistant Attorney General Brian M. Boynton Delivers Remarks at the Federal Bar Association Qui Tam Conference, (Feb. 17, 2021), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-federal-bar. The focus on EHR is consistent with Assistant Attorney General of the United States for the Civil Division Jody Hunt's comments in February 2020 in which she noted that enforcement efforts pertaining to EHR fraud was one of the Department's top three priorities in FCA enforcement for the coming year. Press Release, U.S. Dep't of Justice Assistant Attorney General Jody H. Hunt delivers remarks to the Federal Bar Association 2020 Qui Tam Conference (Feb. 27, 2020), https://www.justice.gov/civil/speech/assistant-attorney-general-jody-h-hunt-delivers-remarks-federal-bar-association-2020.

23. Letter from Christi A. Grimm, Office of Inspector General, U.S. Dep't of Health & Human Srvs., Principal Deputy Inspector General Grimm on Telehealth (Feb. 26, 2021), https://oig.hhs.gov/coronavirus/letter-grimm-02262021.asp.

24. A March 2021 MedPAC report proposed three protections against telemedicine fraud: (1) increased scrutiny for providers that bill a high volume of telehealth services per beneficiary as compared to other clinicians, (2) requiring that clinicians provide an in-person visit before ordering costly DME or clinical laboratory tests, and (3) prohibiting "'incident to' billing for telehealth services provided by any clinician who can bill Medicare directly." *See* Medicare Payment Advisory Comm'n, *Reports to the Congress: Medicare Payment Policy* (Mar. 2021), mar21_medpac_report_to_the_congress_sec.pdf.

25. Colin R. Jennings, *DOJ Pursues More Electronic Health Records Cases*, 9 National Law Review 162 (June 11, 2019), https://www.natlawreview.com/article/doj-pursues-more-electronic-health-records-cases.

In the wake of the Practice Fusion settlement, marketing or brand personnel involvement and/or funding should raise a red flag in the CDS context. Sponsored CDS programs require exacting evaluation to guarantee that they are clinically proper, commercially neutral, and consistent with any pertinent guidelines. CDS tools and other clinical interventions or recommendations must be grounded in evidenced-based medical guidelines.

Telemedicine and EHR technologies have rapidly changed patient care, introducing opportunities for potential fraud and abuse and exposing gaps in oversight. Companies operating in these spaces should expect increased FCA enforcement in these areas going forward and take steps to minimize their risk.

Michael C. Theis
Partner | Denver
+1 303 899 7327
michael.theis@hoganlovells.com

Stacy Hadeka
Counsel | Washington, D.C.
+1 202 637 3678
stacy.hadeka@hoganlovells.com

Michael F. Mason
Partner | Washington, D.C.
+1 202 637 5499
mike.mason@hoganlovells.com

DOJ intensifies scrutiny of cybersecurity practices

On October 6, 2021, Deputy Attorney General Lisa O. Monaco of the Department of Justice (DOJ) announced a Civil Cyber-Fraud Initiative through which DOJ will use the False Claims Act (FCA) to target cybersecurity-related fraud by government contractors and grant recipients.[1] This initiative is part of a Department-wide comprehensive cyber review ordered by Monaco in May. Although it does not impose new regulatory or legal requirements, it signals a new focus and prioritization of resources by DOJ to improve cybersecurity across the government, the public sector, and at key "industry partners."

The initiative also expressly aims to secure FCA recoveries to reimburse the government and taxpayers for losses incurred "when companies fail to satisfy their cybersecurity obligations." Government contractors and grantees should expect increased scrutiny of their compliance with cybersecurity requirements and a corresponding increase in FCA complaints based on alleged failures to meet those obligations. In rolling out this initiative, DOJ has emphasized that civil enforcement will not wait for a cybersecurity breach – cases can be brought for failure to comply with contractual or regulatory requirements even in the absence of such a breach.

Increased focus on contractors and grantees

The initiative is expressly intended to encourage contractors to harden their defenses against computer intrusions, hacks, and cyber-attacks following recent, well-publicized incidents that have highlighted a national security vulnerability. At the same time, several recent, headline-grabbing FCA claims against government contractors have been based on an alleged failure to comply with contract and regulatory cybersecurity requirements or on alleged misrepresentation of such compliance. DOJ settled its first such case in 2019.[2] It and other similar cases have put government contractors on notice that the threat of FCA litigation for non-compliance with cybersecurity measures is real.[3]

Although government contractors have long been prime targets for FCA whistleblowers, this new DOJ initiative further elevates this risk.[4] The emphasis by

1. *See Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative*, U.S. Dep't of Justice (Oct. 6, 2021), available at https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.
2. Joseph Marks, Cisco to Pay $8.6 Million Fine for Selling Government Hackable Surveillance Technology, Wash. Post (July 31, 2019), available at https://www.washingtonpost.com/politics/2019/07/31/cisco-pay-million-fine-selling-government-hackable-surveillance-technology/.
3. *See, e.g., United States ex rel. Adams v. Dell Computer Corp.*, 496 F. Supp. 3d 91 (D.D.C. 2020); *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 3d 1240 (E.D. Cal. 2019).
4. *See* John Hewitt Jones, DOJ expects whistleblowers to play 'significant role' in False Claims Act cases against contractors, FEDScoop (Oct. 13, 2021), available at https://www.fedscoop.com/doj-expects-whistleblowers-to-play-significant-role-in-false-claims-act-cases-against-contractors/.

DOJ on these issues suggests that it may be more prone to intervene in whistleblower cases based on cybersecurity compliance, and this fact may incentivize more whistleblowers to come forward. It will also cause some would-be whistleblowers – who are most often employees and insiders – to examine more closely their companies' cybersecurity obligations and practices. Finally, the initiative will draw government scrutiny not just from DOJ, but also from inspectors general at numerous government agencies who could in turn refer cases to DOJ.

The cybersecurity obligations that could give rise to a claim

Government contractors and grantees are frequent targets for cyberattacks due to their need to store sensitive technical data and other high-value national security information as part of their work. In recognition of this fact, the federal government has imposed a framework of cybersecurity requirements that typically require government contractors and grantees to make substantial investments in data security infrastructure that meet specific standards.

Although FCA claims relating to cybersecurity obligations could take many forms, two recently modified regulatory requirements are noteworthy.

First, in addition to the safeguarding and cyber incident reporting requirements in Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, the Department of Defense (DoD) now requires contractors (through DFARS 252.204-7020) to complete a pre-award assessment of their compliance with cybersecurity controls identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171.[5] This self-assessment is referred to as a "Basic Assessment." It results in a numerical score and must also identify a date by which the contractor will be fully compliant with NIST SP 800-171. Should the validity of a contractor's self-assessment be later questioned, a whistleblower could claim that false or reckless representations made in the self-assessment caused false claims to be made.

Significantly, a Basic Assessment may be followed by a government-led assessment – either a "Medium Assessment" or a "High Assessment" – after award. This could lead to disagreements about the degree to which the contractor is compliant with NIST SP 800-171, and such disagreements could give rise to FCA suits.

Second, through the Cybersecurity Maturity Model Certification (CMMC) program, DoD anticipates the use of self-attestation, third-party certification, and government-led assessments for cybersecurity compliance. When such certification begins, it is possible that third-party certifiers or DoD may uncover inconsistencies between their own assessment of the contractor's security controls and the contractor's earlier

5. Ron Ross, Victoria Pillitteri, Kelley Dempsey, Mark Riddle, & Gary Guissanie, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST SP 800-171 Rev. 2, (Feb. 2020), available at https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

Basic Assessment. Whistleblowers could point to such inconsistencies to allege a contractor caused false claims to be made by misrepresenting its security controls in order to win the contract.

The above DFARS clauses apply only to Controlled Unclassified Information (CUI) within the DoD supply chain. However, numerous government contracts contain contract-specific cybersecurity requirements, and noncompliance with these requirements could also give rise to FCA claims. Furthermore, the Federal Acquisition Regulation (FAR) clause 52.204-21 requires all contractors and subcontractors to apply specified safeguarding requirements when processing, storing, or transmitting Federal Contract Information (FCI) in or from covered contractor information systems.

Finally, we expect additional government-wide cybersecurity standards and reporting requirements to be issued pursuant to EO 14028, which will increase the avenues for potential FCA claims. In addition, if proposals for new legislation and/or regulations that would strengthen cyber incident reporting obligations are implemented, the government will have new avenues for learning of cyber incidents.

Subcontractors should also take note

The FCA imposes liability not only on a prime contractor or direct grant recipient, but it applies to any entity, including subcontractors, whose conduct causes a false claim to be presented to the United States for payment or approval. Although prime contractors or grant recipients typically submit claims for payment directly to the government on behalf of their subcontractors, a subcontractor that causes a prime contractor or recipient to present a false claim for payment can be held liable for FCA damages and penalties.[6]

What's next?

The Supreme Court has noted that the FCA is not a "vehicle for punishing garden-variety breaches of contract or regulatory violations."[7] What remains to be seen is the extent to which suits that allege a failure to comply with fast-developing cybersecurity requirements will meet the rigorous "materiality" requirements outlined by the Supreme Court.[8] The government's intent to bolster security of its supply chain is clear, but federal contracts incorporate dozens of regulatory requirements, and strict compliance with any single one may not be material to the contracting agency's decision to pay for goods or services in every case.

6. *See* 31 U.S.C. § 3729(a)(1); *United States v. Bornstein*, 423 U.S. 303, 309 (1976) ("It is settled that the Act . . . gives the United States a cause of action against a subcontractor who causes a prime contractor to submit a false claim to the Government.").
7. *Universal Health Servs., Inc. v. United States ex rel. Escobar*, 579 U.S. 176, 194 (2016).
8. *Id.* at 194-95, 195 n.6.

Separately, it will be important to watch the cases that arise in this area to see whether the government will seek, and whether the courts will award, damages based upon the full value of the contract or grant, or whether the more traditional "benefit-of-the-bargain" measure of damages will be imposed based upon the difference in value between what the government paid for, and what it received. In some cases you can expect DOJ to contend that the larger measure of damages is appropriate, because the government would never have been induced to award a contract to a company that misrepresented its ability to comply with rigorous cybersecurity requirements.

Despite questions about the strength of future FCA claims based on alleged non-compliance with cybersecurity requirements, companies that contract with the government or receive grants should carefully track fast-evolving cybersecurity rules and regulations and prioritize related compliance efforts.

Jonathan Diesenhaus
Partner | Washington, D.C.
+1 202 637 5416
jonathan.diesenhaus@hoganlovells.com

Matthew C. Sullivan
Partner | New York
+1 212 918 3084
matthew.sullivan@hoganlovells.com

Claudia L. Pare
Senior Associate | Washington, D.C.
+1 202 637 6572
claudia.pare@hoganlovells.com

Fact-intensive materiality inquiries protract litigation

This past year marks the fifth anniversary of the Supreme Court's 2016 decision in *Universal Health Services, Inc. v. United States ex rel. Escobar*, in which the Court articulated the False Claims Act's (FCA) materiality requirement – that is, whether an alleged misrepresentation was capable of influencing the government's payment decision – requires a "demanding" and "rigorous" review that can consider government action in the face of the alleged or similar misrepresentations.[1]

At first, the *Escobar* decision, and its heightened materiality standard, appeared to transform the landscape of FCA enforcement. Case law developed rapidly in its wake, as lower courts grappling with its meaning and application treated similar scenarios differently. More recently, however, the case law has begun to approach an equilibrium – courts will take a "holistic"[2] view of the circumstances of each case, including government (in)action despite knowledge of alleged misconduct, and under which no single fact is dispositive. Because materiality thus is such a fact-intensive inquiry, it has proven to be an issue unlikely to be decided on a motion to dismiss or even, at least in some circumstances, at summary judgment. This is often true despite the Supreme Court's stated view that "materiality is [not] too fact intensive for courts to dismiss [FCA] cases on a motion to dismiss or at summary judgment."[3] Several cases from the past year are illustrative.

Materiality on motion to dismiss: "Many things" could explain the government's continued payment

A split panel of the Seventh Circuit permitted a previously dismissed case to proceed after concluding the relator had sufficiently pled materiality even under heightened fraud-pleading standards.[4] In *U.S. ex rel. Prose v. Molina Healthcare of Illinois, Inc.*, the relator alleged Molina Healthcare had contracted with the Illinois Medicaid program to provide multiple tiers of medical service with scaled capitation rates.[5] The complaint alleged that the highest capitation rate applied to Skilled Nursing Facility

1. *Universal Health Servs., Inc. v. United States ex rel. Escobar (Escobar)*, 579 U.S. 176, 192-93, 195 n.6 (2016).
2. A "holistic" test "with no one factor being necessarily dispositive" was the First Circuit's gloss on its new mandate in the remanded case. *United States ex rel. Escobar v. Universal Health Servs.*, Inc., 842 F.3d 103, 109 (1st Cir. 2016).
3. *Escobar*, 579 U.S. at 195 n.6.
4. No. 20-2243, 2021 WL 5298012, at *8 (7th Cir. Nov. 15, 2021). The Seventh Circuit originally issued the opinion in August 2021, 10 F.4th 765, 776 (7th Cir. 2021), but amended the opinion slightly in November 2021 after voting to deny rehearing and rehearing *en banc*, No. 20-2243, 2021 WL 5296454, at *1 (7th Cir. Nov. 15, 2021).
5. No. 20-2243, 2021 WL 5298012, at *1 (7th Cir. Nov. 15, 2021).

(SNF) services that Molina subcontracted to a third party, GenMed, to deliver.[6] After a dispute caused GenMed to terminate the contract, Molina allegedly did not inform the state it had ceased providing SNF services.[7] The district court found that provision of SNF services was material to the state's payment, but dismissed the complaint after concluding the relator had insufficiently pled Molina's knowledge of that materiality.[8]

The Seventh Circuit, over a strong dissent,[9] disagreed and reversed, concluding the complaint plausibly alleged that "as a sophisticated player in the medical-services industry, Molina was aware that [SNF] services play a material role in the delivery of Medicaid benefits."[10] The court recognized that Molina's "strongest argument against materiality" was that the government continued to contract with Molina after learning it could no longer provide SNF services even renewing its contract twice after the suit was filed.[11] That argument, however, was "better saved for a later stage, once both sides have conducted discovery" and "[l]ater exploration will be needed before anyone can say what the government did and did not know about Molina's provision of SNF services."[12] In the meantime, the court concluded Molina's assertion that the government was aware of all material facts is not enough to dismiss the relator's claim and that "[m]any things could explain the government's continued contracting with Molina."[13]

The D.C. Circuit reversed a district court's dismissal of a suit in a similar manner. In *Cimino v. Int'l Bus. Machines Corp.*, the lower court had ruled that the relator failed to plausibly allege materiality in a situation where the defendant used an allegedly inaccurate audit of software license usage in a contract negotiation with the IRS. The lower court had noted that the IRS continued making payments pursuant to the agreement that was allegedly fraudulently induced after learning of the alleged fraud and even exercised options extending the agreement despite that knowledge.[14] In reversing, the D.C. Circuit explained the IRS could have continued to pay for "any number of reasons" that did not render the alleged fraud immaterial.[15] The court acknowledged that later evidence could demonstrate the alleged fraud was not material to the IRS, but that was "for another day."[16] In the same decision, however, the D.C. Circuit held that to prevail on a fraudulent inducement theory of liability (the only theory remanded for further litigation), the relator would have to show that the allegedly fraudulent inaccuracies in the audits supplied to the IRS were the "but for" cause of the agency awarding IBM the new contract.

6. *Id.*
7. *Id.*
8. *Id.*
9. Chief Judge Sykes in dissent accused the majority of disregarding both *Escobar* and Seventh Circuit precedent and would have affirmed dismissal of the complaint. *Id.* at *9-10.
10. *Id.* at *1, *8-9.
11. *Id.* at *7.
12. *Id.*
13. *Id.*
14. *Cimino v. Int'l Bus. Machines Corp.*, No. 13-CV-00907 (APM), 2019 WL 4750259, at *7 (D.D.C. Sept. 30, 2019), *aff'd in part, rev'd in part and remanded sub nom. United States ex rel. Cimino v. Int'l Bus. Machines Corp.*, 3 F.4th 412 (D.C. Cir. 2021).
15. *United States ex rel. Cimino v. Int'l Bus. Machines Corp.*, 3 F.4th 412, 423 (D.C. Cir. 2021).
16. *Id.*

Materiality at summary judgment: The significance of continued government payment "may vary depending on circumstances"

In yet another important case on the issue of materiality, the Eleventh Circuit held that the "significance of continued payment may vary depending on the circumstances."[17] Bibby involved allegations by mortgage brokers that mortgage lenders were charging fees that were prohibited by the Department of Veterans Affairs (VA) regulations by bundling them with permitted fees[18] while expressly certifying they charged only permissible fees. The defendant moved for summary judgment, which the district court granted after noting "the stringent materiality standard espoused by the Supreme Court chokes the life out of Relators' case and mandates the end of this action."[19] In so ruling, the district court cited the fact that despite VA audits revealing the prohibited fees, the VA took no heightened action against the defendant other than requiring it to refund improper fees and continued to issue loans.[20]

The relators appealed, arguing – along with the government as amicus curiae – that the VA's continued payment "merit[ed] little weight because the payments were required by law."[21] The Eleventh Circuit agreed. Absent a dispute regarding the VA's actual knowledge of the defendant's violation of VA regulations, the court looked to the VA's reaction to that knowledge.[22] And while the court acknowledged that, under Escobar, the "government action relevant to the materiality inquiry is typically the payment decision," because the VA was statutorily bound to honor the payments, the "facts of this case" required the court to "cast [its] materiality inquiry more broadly" to consider "the full array of tools at the VA's disposal for detecting, deterring, and punishing false statements, and which of those it employed."[23] After "looking at the VA's behavior holistically," the court described a number of actions taken by the VA to address noncompliance with fee regulations, including releasing a circular to lenders on the consequences of noncompliance, implementing more audits, and requiring lenders to refund any improperly charged fees.[24] Because the VA "did take some enforcement actions" even though it "did not take the strongest possible action" against the defendant, sufficient evidence of materiality was present.[25] The ultimate determination of materiality was a question for the factfinder.[26]

17. *United States ex rel. Bibby v. Mortg. Invs. Corp.*, 987 F.3d 1340, 1350 (11th Cir. 2021), cert. denied sub nom. Mortg. Invs. Corp. v. United States ex rel. Bibby, 141 S. Ct. 2632 (2021).
18. *Id.* at 1343-45.
19. *United States ex rel. Bibby v. Mortg. Invs. Corp.*, Civ. Action No. 12-CV-4020-AT, 2019 WL 11637354, at *2 (N.D. Ga. July 1, 2019).
20. *Id.* at *26 (noting "rampant noncompliance" and the VA's "laissez faire attitude in dealing with the problem"), *29.
21. *Bibby*, 987 F.3d at 1350.
22. *Id.*
23. *Id.* (internal citations omitted).
24. *Id.* at 1350-52.
25. *Id.* at 1352.
26. *Id.*

Proposed legislation attempts to limit materiality defenses

In July 2021, Senator Grassley, and a bipartisan group of co-sponsors, proposed amending the FCA to make it more difficult and burdensome for defendants to argue the government or relator failed to prove materiality.[27] Specifically, the proposed amendment would establish new procedures for litigating materiality by permitting the government or relator to establish materiality by a "preponderance of evidence" while a defendant could only rebut materiality through "clear and convincing evidence." The amendment would also make it harder for defendants to secure the necessary discovery from government agencies. Citing "confusion" and "fallout" from *Escobar*, the bill's sponsors claim the proposed amendment would help "recoup even more" "lost taxpayer dollars" and help "ensur[e] that those who defraud the federal government are held accountable."[28]

Since its introduction, and after receiving criticism, Senator Grassley introduced a "manager's amendment" to the bill.[29] The revised language removes, among other things, the burden-shifting language. The bill now states "In determining materiality, the decision of the Government to forego a refund or pay a claim despite actual knowledge of fraud or falsity shall not be considered dispositive if other reasons exist for the decision of the Government with respect to such refund or payment."[30] The amendment is still intended to "correct" "misinterpretation" by the courts that "gut" and do a "disjustice [sic] to the original purpose" of the FCA[31] while seeming to endorse another line of case law that looks to other reasons the government might continue paying during the materiality inquiry, like the courts did recently in *Prose* and *Cimino* and going back a few years in *Campie*.[32]

The Senate Judiciary Committee voted the bill out of committee on October 28, 2021, and it awaits a vote by the Senate.[33]

* * *

Absent legislative action, case developments from the past year reaffirm the extent to which materiality will remain a fact-intensive, case-by-case inquiry – and one that parties to FCA litigation may find resolved only late in the litigation process.

27. *See* S5776, 117 Cong. Rec. (Aug. 3, 2021), https://www.congress.gov/117/crec/2021/08/03/167/138/CREC-2021-08-03-pt1-PgS5726.pdf. Senator Grassley also proposed the same changes in the standalone "False Claims Act Amendment of 2021," introduced on July 22, 2021, as S.2428, https://www.congress.gov/117/bills/s2428/BILLS-117s2428is.pdf.

28. *Senators Introduce Bipartisan Legislation to Fight Government Waste, Fraud*, Grassley.senate.gov (July 26, 2021), https://www.grassley.senate.gov/news/news-releases/senators-introduce-of-bipartisan-legislation-to-fight-government-waste-fraud.

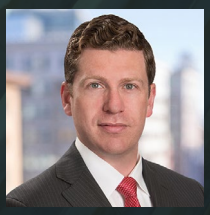
29. *Executive Business Meeting*, Senate Comm. on the Judiciary, 117th Cong. (Oct. 21, 2021), https://www.judiciary.senate.gov/meetings/10/14/2021/executive-business-meeting.

30. *Draft Copy of ALB21G65 FMS*, Senate Legis. Counsel, S.2428, 117 Cong. (Oct. 19, 2021), https://g7x5y3i9.rocketcdn.me/wp-content/uploads/2021/10/Managers-Amendment-pdf.pdf.

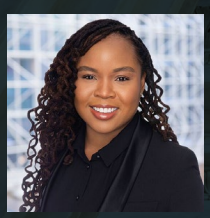
31. *Executive Business Meeting*, Senate Comm. on the Judiciary, 117th Cong. (Oct. 21, 2021), https://www.judiciary.senate.gov/meetings/10/14/2021/executive-business-meeting.

32. *See, e.g., United States ex rel. Campie v. Gilead Scis., Inc.*, 862 F.3d 890, 906 (9th Cir. 2017) (relator sufficiently alleged materiality reasoning, in part, that it would be a mistake to "read too much into the FDA's continued approval" and that "there are many reasons the FDA may choose not to withdraw a drug approval, unrelated to the concern that the government paid out billions of dollars for nonconforming and adulterated drugs").

33. False Claims Amendments Act of 2021, S. 2428, 117th Cong. (2021-2022), Congress.gov, https://www.congress.gov/bill/117th-congress/senate-bill/2428/text?q=%7B%22search%22%3A%5B%22False+Claims+Act%22%5D%7D&r=1&s=1(last visited on Dec. 1, 2021).



David I. Sharfstein
Partner | Washington, D.C., Baltimore
+1 202 637 5739 (Washington, D.C.)
+1 410 659 2721 (Baltimore)
david.sharfstein@hoganlovells.com



Jennifer Hill
Associate | Washington, D.C.
+1 202 804 7831
jennifer.hill@hoganlovells.com

Standard for government dismissals remains uncertain

In our 2020 and 2021 editions of our False Claims Act (FCA) guide, we noted recent developments relating to the United States Department of Justice's (DOJ) authority under 31 U.S.C. §3730(c)(2)(A) to seek dismissal of suits filed under the qui tam provisions of the FCA. Beginning with the Granston Memo in 2018, which DOJ later incorporated into the Justice Manual, increased attention on the legal standard governing such motions to dismiss gave rise to a circuit split. That split widened in 2020 with the emergence of yet a third standard, and more so over the last year with additional case law interpreting the existing standards, and legislation introduced in the U.S. Senate that could limit DOJ's control over qui tam litigation in significant ways.

The *Swift / Sequoia* circuit split

Going back almost 20 years, there has been a circuit split governing the standard applied to DOJ motions to dismiss suits filed under the qui tam provisions of the FCA where the government has declined to intervene. The D.C. Circuit "give[s] the government an unfettered right to dismiss an action," rendering the government's decision to dismiss essentially "unreviewable," under its opinion in *Swift v. United States*.[1] The Eighth Circuit has suggested a similar standard, noting that a government's power to dismiss over relator's objection is "subject only to notice and a hearing for the qui tam relator."[2] However, courts in the Ninth and Tenth Circuits apply the standard from *United States ex rel. Sequoia Orange Co. v. Baird-Neece Packing Corp.*, which requires the government to demonstrate a valid purpose for dismissal and a "rational relation" between dismissal and accomplishment of that purpose.[3]

The *CIMZNHCA* decision

As noted in our 2021 FCA Guide, just after the Supreme Court declined in April 2020 to resolve the existing circuit split arising from the *Swift* and *Sequoia* standards,[4] a third

1. 318 F.3d 250, 252-53 (D.C. Cir. 2003).
2. *See United States ex rel. Rodgers v. Ark.*, 154 F.3d 865, 868 (8th Cir. 1998).
3. 151 F.3d 1139, 1145 (9th Cir. 1998). *See Ridenour v. Kaiser–Hill Co., L.L.C.*, 397 F.3d 925, 940 (10th Cir. 2005).
4. *United States ex rel. Borzilleri v. AbbVie, Inc.*, 837 F. App'x 813 (2d Cir. 2020). On April 6, 2020, the Supreme Court denied a petition for certiorari that could have provided an opportunity for the Court to clarify the standard for DOJ dismissal. *See United States ex rel. Schneider v. JP Morgan Chase Bank NA*, 140 S. Ct. 2660 (2020) in the Supreme Court of the United States. See also Mike Theis & Stacey Hadeka, The *CIMZNHCA* decision: A third standard for DOJ dismissals, https://fca-2021.hoganlovellsabc.com/2020-and-the-road-ahead/lessons-from-polansky-the-continuing-assault-on-sub-regulatory-guidance.

standard of review for DOJ dismissals emerged from the Seventh Circuit.[5] In *United States ex rel. CIMZNHCA, LLC v. UCB, Inc. (CIMZNHCA)*, the Seventh Circuit drew from the language in Rule 41(a) of the Federal Rules of Civil Procedure as the basis for deciding the government's dismissal authority.[6] The *CIMZNHCA* decision effectively affords the government a largely unfettered right to intervene and dismiss over the relator's objection during the early stages of litigation, but once the defendant files a responsive pleading, then "an action may be dismissed at the plaintiff's request only by court order, on terms that the court considers proper."[7] Finding the government had a rational basis for moving to dismiss, the Seventh Circuit reversed and remanded to the district court with instructions to enter judgment for the defendants on the relator's claims, dismissing those claims with prejudice as to the relator.[8]

The Third Circuit deepens a three-way circuit split

Following the *CIMZNHCA* decision, in October 2021 the Third Circuit decided to adopt the same FRCP 41(a) standard in *U.S. ex rel Polansky v. Executive Health Resources, Inc.*[9] In *Polansky*, the Relator's claims implicated Medicare reimbursement policy and medical necessity determinations required to justify inpatient admissions over outpatient procedures.[10] In accordance with the qui tam statute, the case remained under seal while DOJ investigated; ultimately DOJ declined to intervene.[11] More than several years after the declination and periods of active litigation, in February 2019, DOJ informed the parties that it intended to dismiss the entire action pursuant to 31 U.S.C. § 3730(c)[12] and filed its motion in August 2019.[13] The district court granted the motion and "concluded that the [g]overnment had made an adequate showing under any of the prevailing standards."[14]

On the plaintiff's appeal, the Third Circuit addressed two questions: (1) does the FCA require the government to intervene in order to seek dismissal pursuant to § 3730(c)(2)(A) – either at the first opportunity[15] or "at a later date upon a showing of good cause"?[16] ; and (2) what is the standard governing the government's motion to dismiss?[17]

5. *United States ex rel. CIMZNHCA, LLC, v. UCB, Inc.*, 970 F.3d 835 (7th Cir. 2020).
6. 970 F.3d at 849-50 (noting that dismissals under Rule 41(a) are "[s]ubject to . . . any applicable federal statute," which imports the limitations articulated in § 3730(c)(2)(A) and concluding the government may dismiss the action without the relator's consent if the relator receives notice and opportunity to be heard as required by § 3730(c)(2)(A)); see also Fed. R. Civ. P. 41(a)(2).
7. 970 F.3d at 849-50.
8. *Id.* at 854.
9. *Polansky v. Exec. Health Res. Inc*, No. 19-3810, 17 F.4th 376 (3d Cir. 2021).
10. *Id.*
11. *Id.*
12. *Id.*
13. *Id.*
14. *Id.*
15. 31 U.S.C. § 3730(c)(2)(A).
16. *Id.* § 3730(c)(3).
17. *Polansky*, 17 F.4th 376 (3d Cir. 2021).

In addressing the procedural question, the Third Circuit held that the government must intervene before it can move to dismiss, and that it can seek leave to intervene at any point in the litigation upon a showing of good cause. The circuit courts are also split on this procedural point, with the Third, Sixth, and Seventh Circuits interpreting the FCA to require intervention before the government can move to dismiss a relator's case[18] and the Ninth, Tenth, and D.C. Circuit's disagreeing.[19]

Turning to the standard governing the government's motion to dismiss, the court followed the Seventh Circuit's reasoning in *CIMZNHCA*, described above. The court held that the government, as an intervenor,[20] is subject to F.R.C.P. 41(a), which articulates the standard the government must meet for a dismissal. Applying this standard, the Third Circuit affirmed the district court's decision to grant the government's motion to dismiss. Beyond the immediate dispute at issue, the *Polansky* decision creates further discord among the circuits about the standard for a motion to dismiss under § 3730(c)(2)(A), and it puts a brighter spotlight on the circuits that have not yet addressed the issue.[21]

Potential legislative response

With the Supreme Court only recently having declined to address the circuit split, Senator Charles Grassley has tried to take legislative action. In July 2021, Senator Grassley introduced a bill (S 2428 – False Claims Amendments Act of 2021) that addresses the standard for DOJ's dismissal authority head on, and effectively adopts the *Sequoia Orange* standard followed in the Ninth and Tenth Circuits. The bill proposes to amend § 3730(c)(2)(A) to read as follows: "The Government may dismiss the action notwithstanding the objections of the person initiating the action if the person has been notified by the Government of the filing of the motion and the court has provided the person with an opportunity for a hearing on the motion, *at which the Government shall identify a valid government purpose and a rational relation between dismissal and accomplishment of the purpose, and the person initiating the actions shall have the burden of demonstrating that the dismissal is fraudulent, arbitrary and capricious, or illegal."*[22] The bill has advanced through the Senate Judiciary Committee, but the full Senate has not yet voted on it.[23]

18. *Id.*; *CIMZNHCA*, 970 F.3d at 844 (7th Cir. 2020) (interpreting the FCA to require intervention upon a showing of good cause before the Government can move to dismiss a relator's case under § 3730(c)(2)(A) but treating the government's motion to dismiss as both a motion intervene and a motion to dismiss); and *United States ex rel. Poteet v. Medtronic, Inc.*, 552 F.3d 503, 519-20 (6th Cir. 2009) (concluding § 3730(c)(2)(A) "applies only when the government has decided to 'proceed[ ] with the action'" (quoting § 3730(c)(1)), *abrogated on other grounds by United States ex rel. Rahimi v. Rite Aid Corp.*, 3 F.4th 813 (6th Cir. 2021).

19. *Ridenour v. Kaiser-Hill Co.*, 397 F.3d 925, 934-35 (10th Cir. 2005) (holding the Government "is not required to intervene . . . before moving to dismiss the action under § 3730(c)(2)(A)"); *Swift v. United States*, 318 F.3d 250, 252 (D.C. Cir. 2003) (reaching the same conclusion); and *United States ex rel. Sequoia Orange Co. v. Baird-Neece Packing Corp.*, 151 F.3d 1139, 1145 (9th Cir. 1998) (suggesting the same understanding).

20. The government did not formally intervene as a party. However, the court decided that there was no cause for remand on the basis of the record. The court reasoned, "we construe the Government's motion to dismiss as including a motion to intervene because intervention was in substance what the government sought and in form what the False Claims Act requires." *Polansky*, 17 F.4th 376 (3d Cir. 2021) (internal citations omitted).

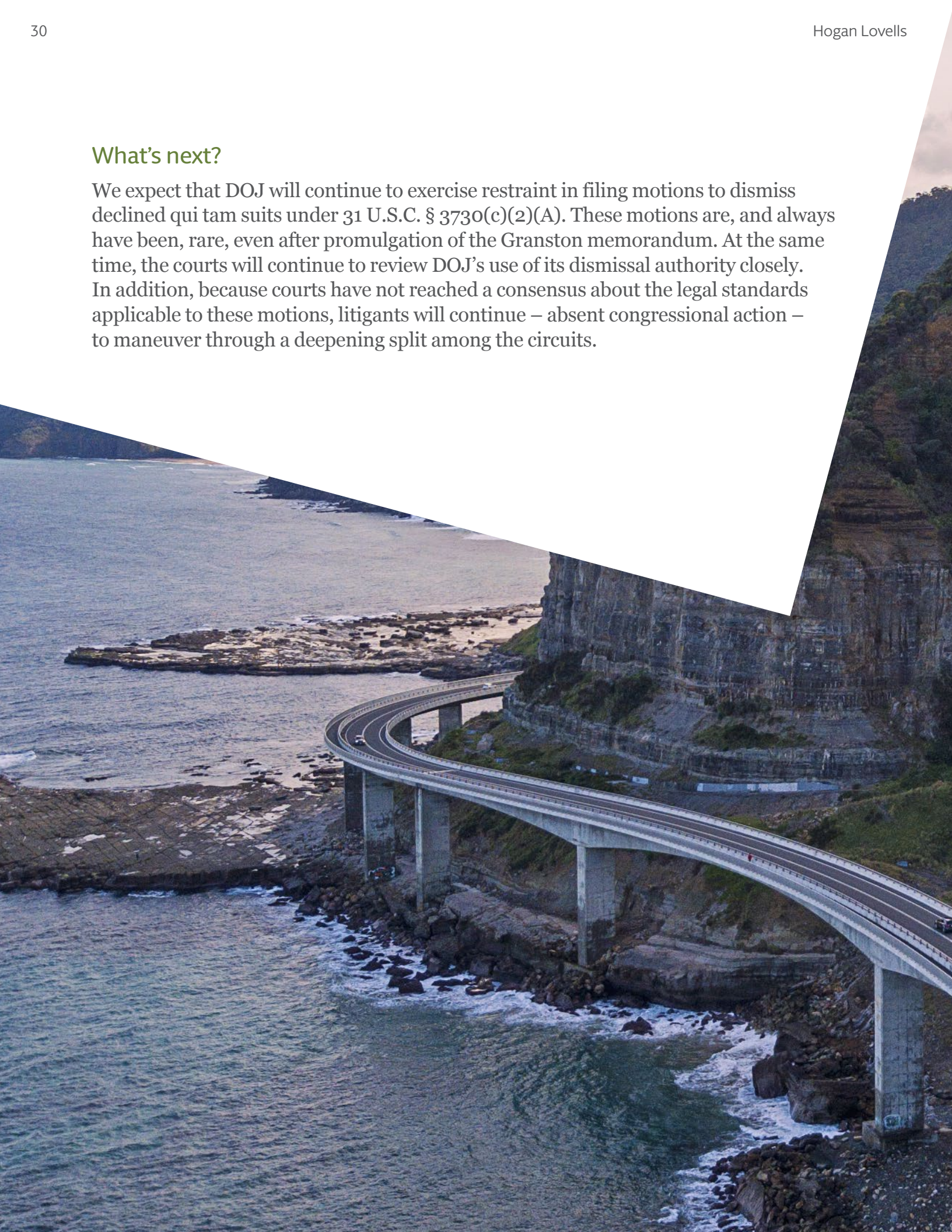
21. In July 2021, the Fifth Circuit, while affirming the district court's decision to grant the Government's motion to dismiss, declined to decide the proper judicial standard of review for DOJ dismissals. *United States v. Eli Lilly & Co., Inc.*, 4 F.4th 255, 267-69 (5th Cir. 2021).

22. 31 U.S.C. § 3730(c)(2)(A); False Claims Amendments Act of 2021, S.2428, 117th Cong. (2021) https://www.congress.gov/bill/117th-congress/senate-bill/2428/text.

23. *Id.*

What's next?

We expect that DOJ will continue to exercise restraint in filing motions to dismiss declined qui tam suits under 31 U.S.C. § 3730(c)(2)(A). These motions are, and always have been, rare, even after promulgation of the Granston memorandum. At the same time, the courts will continue to review DOJ's use of its dismissal authority closely. In addition, because courts have not reached a consensus about the legal standards applicable to these motions, litigants will continue – absent congressional action – to maneuver through a deepening split among the circuits.



Jonathan Diesenhaus
Partner | Washington, D.C.
+1 202 637 5416
jonathan.diesenhaus@hoganlovells.com

Rob Beecher
Associate | Philadelphia
+1 267 675 4692
rob.beecher@hoganlovells.com

Safeco, *Supervalu*, and objectively reasonable interpretations of ambiguous regulations

The Supreme Court's decision in *Safeco*[1] has been widely applied by circuit courts to hold that a defendant does not "recklessly disregard [] the truth or falsity" of its claims for the purposes of False Claims Act (FCA) scienter when that defendant operates under an "objectively reasonable" interpretation of the prevailing regulatory scheme. But *Safeco*'s application to the other portions of the FCA's scienter definition are still being debated by the lower courts. Two decisions handed down in 2021, the Seventh Circuit decision in *Supervalu*[2] and the D.C. District Court decision in *Norton*[3], highlight the diverging approach to how far *Safeco*'s analysis extends. Indeed, the hotly debated decision in *Supervalu* may give the Supreme Court an opportunity to answer the underlying question itself.

Background on *Safeco* and FCA scienter

The FCA prohibits only the "knowing[]" misconduct involving submission of false claims to the government.[4] Time and again, Congress, courts, and the Justice Department point to this element as the critical factor separating mere regulatory non-compliance from misconduct punishable under the FCA.[5] The statute defines "knowing" and "knowingly" with three sub-divisions, to mean "actual knowledge of the [falsity,]" "act[ing] in deliberate ignorance of the truth or falsity of the information," "or" "act[ing] in reckless disregard of the truth or falsity of the information[.]"

The Supreme Court's decision in *Safeco* involved the Fair Credit Reporting Act, rather than the FCA. That statute imposes liability when the defendant "willfully fails to comply" with its requirements. The Supreme Court agreed that "willful" acts could be those made with a "reckless disregard" for the statute, but held that a defendant does not act with recklessness when operating under an interpretation of the statute that is not "objectively unreasonable." Because the FCA also includes "reckless disregard" in its statutory definition of "knowing", several circuits courts have applied *Safeco* to the "reckless disregard" prong of FCA scienter.[6]

1. *Safeco Ins. Co. of Am. v. Burr*, 551 U.S. 47, 47 (2007).
2. *United States ex rel. Schutte v. Supervalu Inc.*, 9 F.4th 455 (7th Cir. 2021).
3. *United States ex rel. Morsell v. NortonLifeLock, Inc.*, No. CV 12-800 (RC), --- F. Supp. 3d ----, 2021 WL 3363446 (D.D.C. Aug. 3, 2021) (reconsideration of previous order denying defendant's motion for summary judgment).
4. 31 USCA § 3729.
5. *See, e.g., Universal Health Servs., Inc. v. United States ex rel. Escobar (Escobar)*, 579 U.S. 176, 191-92 (2016).
6. *See also United States ex rel. Streck v. Allergan, Inc.*, 746 F. App'x 101, 106 (3d Cir. 2018); *United States ex rel. McGrath v. Microsemi Corp.*, 690 F. App'x 551, 552 (9th Cir. 2017); *United States ex rel. Donegan v. Anesthesia Assocs. of Kan. City, PC*, 833 F.3d 874, 879–80 (8th Cir. 2016); *United States ex rel. Purcell v. MWI Corp.*, 807 F.3d 281, 284 (D.C. Cir. 2015). Since the Seventh Circuit's decision in *Supervalu*, the Fourth Circuit has joined in holding that *Safeco*'s objectively reasonable standard applies to the FCA. *See U.S. ex rel. Sheldon v. Allergan Sales, LLC*, --- F.4th ---- (2022), 2022 WL 211172 at *1 (4th Cir. Jan. 25, 2022)

Supervalu and the Seventh Circuit's view of *Safeco*

On August 12, 2021, the Seventh Circuit issued its decision in Supervalu, becoming the fifth circuit to expressly apply *Safeco* to the FCA. At issue in Supervalu was the defendant's interpretation of "usual and customary charges[.]" Affirming the district court's grant of summary judgment, the Seventh Circuit agreed that *Supervalu* had put forth an objectively reasonable interpretation of the applicable authority under *Safeco*.

The Seventh Circuit decision lays out a two-part test for determining whether *Safeco* precludes a finding of "knowing" misconduct in the context of an ambiguous regulation: "whether the defendant has a permissible interpretation of the relevant provision and whether authoritative guidance nevertheless warned it away from that reading." In doing so, the Seventh Circuit took a broad approach to whether the proffered interpretation was permissible, noting that the *Safeco* standard "tethered the objectively reasonable inquiry to the legal text, not its underlying policy," and rejected an argument that a "clear purpose" for a statute or regulation foreclosed any finding of ambiguity permitting an alternative, permissible interpretation.

In an unusually combative back and forth, the *Supervalu* majority dueled with a dissent over the time at which the defendant became aware of the alternative, objectively reasonable interpretation. The dissent sought to impose a limitation that, in order to foreclose any finding that it had acted "recklessly," the defendant must show that it held the objectively reasonable interpretation "at the time it submitted its false claim," expressing a concern that defendants would rely on an alternative interpretation that was manufactured post hoc as a way to avoid liability. In such a case, the dissent posited, the defendant would have acted with subjective bad faith, which is "central" to common law fraud, and applicable to the "actual knowledge" prong of FCA scienter. The dissent expressed concern that the standard articulated presented far too narrow a view of the FCA's scienter requirement, and that the majority's "bottom line" was that "only objectively reckless disregard matters, and subjective bad faith does not[.]"

The *Supervalu* majority engaged with these points, ultimately holding that FCA liability is foreclosed when the *Safeco* standard is not met. The *Supervalu* majority's rejoinder to the dissent characterizes it as a distinction between what the defendant "knows" versus what it "believes." As the majority's argument goes, if there is an objectively reasonable alternative interpretation of the applicable authority, even one not held by the defendant at the time the claim was submitted, then the defendant might "believe" that it was submitting a false claim, but it could not "know" it was doing so. In this way, the *Supervalu* majority supported its view that an objectively reasonable interpretation of the statute precluded a finding of FCA scienter under any of the additional textual prongs.

This broad "safe harbor" for FCA liability prompted an immediate challenge. Both the Department of Justice and the organized Relators' bar, through the Taxpayers Against Fraud Education Fund, filed amicus briefs in support of the relators' petition for the Seventh Circuit's en banc review of *Supervalu*. The government argued that a defendant's subjective and correct "belief" that it was violating the statute is sufficient to establish that they acted "knowingly" even when they later identified an alternative, reasonable interpretation consistent with their conduct.[7] Echoing the Supervalu dissent, the government argued that the *Supervalu* majority erred by focusing only on whether an alternative interpretation was "objectively reasonable[,]" in disregard of the alternative scienter prongs and their roots in common law fraud[8]. Although the Seventh Circuit denied the petition for en banc review on December 3, 2021,[9] the controversy seems unlikely to end without the relator seeking further review on petition for certiorari before the Supreme Court.

The alternative approach in *Norton*

The recent *Norton*[10] decision by Judge Contreras of the U.S. District Court for the District of Columbia reflects the dueling application of *Safeco* to FCA scienter. Although *Norton* involved no dispute over whether *Safeco*'s objectively reasonable standard applied, it focused on the timing issue that surfaced in *Supervalu*. Judge Contreras considered the extent to which an objectively reasonable belief, not held contemporaneous with the submission of the claim, could preclude a finding that the defendant acted "knowingly" under the FCA. Judge Contreras held that neither *Safeco* nor related authority in the D.C. Circuit established that an identification and adoption of a reasonable interpretation after the fact could foreclose a finding of liability.[11]

A particularly noteworthy aspect of the court's analysis in *Norton* is its reconciliation of precedent that stated "subjective intent – including bad faith – is irrelevant when a defendant seeks to defeat a finding of knowledge based on its [objectively] reasonable interpretation of a regulatory term," with its own holding that a reasonable interpretation, discovered post hoc and not held at the time of the allegedly false claim, was also irrelevant to that finding. The opinion suggests that a defendant who adopts an objectively reasonable interpretation of an ambiguous regulation contemporaneous with the submission of a claim, and "hews" to that interpretation through the period covered by that claim, can avoid liability, even if that defendant also suspected the agency receiving the claim might not agree. Under the *Norton* standard, the questions are

7. *United States ex rel. Schutte v. Supervalu Inc.*, No. 20-2241, (7th Cir. Sep. 30, 2021), ECF No. 68.
8. The government also took issue with the majority's discussion of the second prong under the Safeco standard: whether the defendant was "warned away" from the otherwise permissible alternative interpretation. The government argued that *Supervalu* was incorrect that only governmental authority was relevant to this analysis.
9. Order Denying *En Banc* Petition, *United States ex rel. Schutte v. Supervalu Inc.*, No. 20-2241, (7th Cir. Dec. 3, 2021), ECF No. 79.
10. *NortonLifeLock,* 2021 WL 3363446.
11. *Id.* at *9 (quoting *Halo Elecs., Inc. v. Pulse Elecs., Inc.*, ––– U.S. ––––, 136 S. Ct. 1923, 1933 (2016), "culpability is generally measured against the knowledge of the actor at the time of the challenged conduct.").

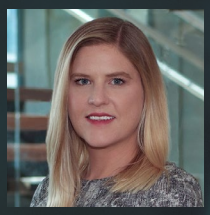
limited to the objective reasonableness of the defendant's proffered exculpatory interpretation and whether it was held at the time the claim was submitted. In this way, the *Norton* case appears to be in conflict with the *Supervalu* decision. To the *Supervalu* court, scienter is akin to a legal impossibility when a defendant's claims are in accord with an objectively reasonable interpretation of an ambiguous provision; to the District Court in *Norton* (as well as the *Supervalu* dissent and DOJ), an additional factual inquiry is necessary to determine if the defendant actually held that objectively reasonable belief at the time the claim was submitted. In *Norton*, the question of when the defendant adopted an objectively reasonable view of the regulation was found to be a question for the jury.[12]

Conclusion

The practical implications of the analytical debate visible in the opinions in *Supervalu* and *Norton* are of great significance to individuals and corporations who operate every day in the context of complex and ambiguous government regulations. Under either view of the timing element, where the government fails to issue guidance clarifying an ambiguous provision, putative FCA defendants who identify and then act on objectively reasonable interpretations of such provisions can seek "safe harbor" under *Safeco*. But a decade after Safeco, other questions remain open, including who bears the burden of proof, what types of evidence show that a defendant held an objectively reasonable belief at a particular point in time, and whether invoking the safe harbor triggers a waiver of the attorney-client privilege.

12. Judge Contreras's opinion is doubly noteworthy because of his familiarity with FCA litigation from his prior work as the Chief of the Civil Division of the United States Attorney's Office of the District of Columbia.

Gejaa Gobena
Partner | Washington, D.C.
+1 202 637 5513
gejaa.gobena@hoganlovells.com



Emily Lyons
Counsel | Washington, D.C.
+1 202 637 6156
emily.lyons@hoganlovells.com

Re-evaluating the benefits of DOJ cooperation

Self-disclosure, cooperation, and remediation: these are three buzz words that have been driving much of U.S. Department of Justice's (DOJ) white-collar enforcement efforts for the last half-decade. While there is no obligation to take any of those steps, the DOJ has offered a variety of incentives with the goal of convincing companies there may be strategic advantages to doing so. Because the False Claims Act (FCA) offers a powerful financial incentive for qui tam relators to file suit on behalf of the government rather than raise their concerns with a company internally, companies facing FCA claims frequently do not have an opportunity to self-disclose. Cooperation is therefore even more important as a means for companies to lessen the size of any potential FCA resolution.

The DOJ recently restored prior guidance requiring that, to be eligible for cooperation credit, companies must provide the DOJ with all non-privileged information about individuals involved in or responsible for the misconduct at issue, regardless of their position, status or seniority. With this change in policy, it is important to outline what actions corporations must take to receive cooperation credit from the DOJ, what reductions the DOJ may implement in return, and whether self-disclosure and cooperation are really worth it.

Who earns cooperation credit in an FCA investigation?

The Justice Manual, which contains a set of internal guidelines that must be considered by DOJ attorneys, identifies three factors that the DOJ considers for purposes of potential "credit that will be provided by [DOJ] attorneys": "when entities and or individuals" (1) "voluntarily self-disclose misconduct that could serve as the basis for False Claims Act (FCA) liability and/or administrative remedies"; (2) "take other steps to cooperate with FCA investigations and settlements"; or (3) "take adequate and effective remedial measures."[1] A closer examination of the contours and impacts of voluntary self-disclosure and cooperation follows.

Voluntary self-disclosure

Companies will receive credit for truly voluntarily disclosures of wrongdoing unknown to the government. When false claims and fraud are "previously unknown" to the government, companies can receive credit for "proactive, timely, and voluntary" self-disclosure of misconduct. According to the guidance in the Justice Manual, disclosure of misconduct[2] allows "the government to make itself whole from[] previously unknown

1. Justice Manual, 4-4.112 - Guidelines For Taking Disclosure, Cooperation, And Remediation Into Account In False Claims Act Matters, U.S. Dep't of Justice (updated April 2018) https://www.justice.gov/jm/jm-4-4000-commercial-litigation#4-4.112.
2. *Id.*

false claims and fraud," and could allow the government "to preserve and gather evidence that would otherwise be lost."[3] In addition, even when the government is aware of certain allegations of potential misconduct, the Justice Manual provides that companies can still receive credit during the course of the investigation for discovering and disclosing to the government "additional misconduct going beyond the scope of the known concerns." [4]

Cooperation

The DOJ also may recognize cooperation absent a voluntary disclosure, especially where they were already investigating claims brought under the FCA qui tam provisions or if the company has not completed its internal investigation. According to the Justice Manual, there is no comprehensive list of what constitutes cooperation in the eyes of the DOJ, but they have provided the following examples of non-mandatory measures that may be "taken into account" in determining whether a company has cooperated:

- Identifying individuals substantially involved in or responsible for the misconduct;
- Disclosing relevant facts and identifying opportunities for the government to obtain evidence relevant to the government's investigation that is not in the possession of the entity or individual or not otherwise known to the government;
- Preserving, collecting, and disclosing relevant documents and information relating to their provenance beyond existing business practices or legal requirements;
- Identifying individuals who are aware of relevant information or conduct, including an entity's operations, policies, and procedures;
- Making available for meetings, interviews, examinations, or depositions an entity's officers and employees who possess relevant information;
- Disclosing facts relevant to the government's investigation gathered during the entity's independent investigation (not to include information subject to attorney-client privilege or work product protection), including attribution of facts to specific sources rather than a general narrative of facts and providing

3. *Id.*
4. *Id.*

timely updates on the organization's internal investigation into the government's concerns, including rolling disclosures of relevant information;

- Providing facts relevant to potential misconduct by third-party entities and third-party individuals;
- Providing information in native format, and facilitating review and evaluation of that information if it requires special or proprietary technologies so that the information can be evaluated;
- Admitting liability or accepting responsibility for the wrongdoing or relevant conduct; and
- Assisting in the determination or recovery of the losses caused by the organization's misconduct.[5]

The DOJ values this type of proactive aid because it increases DOJ efficiencies and reduces the burden on DOJ attorneys, provides access to information and witnesses otherwise not known to the government, and assists the DOJ in identifying the root causes of potential violations and the individuals responsible.

Regarding the first measure – identifying individuals responsible or involved – on October 28, 2021, Deputy Attorney General (DAG) Lisa O. Monaco gave a speech emphasizing accountability and announcing the DOJ's restoration of prior guidance that requires companies to provide the DOJ with all non-privileged information about individuals involved in or responsible for the misconduct at issue, regardless of their position, status, or seniority, in order to be eligible for cooperation credit.[6] This is in contrast to the May 7, 2019, guidelines released by the DOJ during the Trump administration, which previously eased the threshold for receiving cooperation credit to allow for it where a company disclosed information about individuals "substantially involved."[7]

DAG Monaco explained that companies must once again provide "all non-privileged information about individuals involved in or responsible for the misconduct at issue" because the previous guidelines were "confusing" and allowed cooperating companies too much latitude and discretion with reporting requirements. Of course, there is an argument that the constantly changing policies and reintroduction of broad, undefined cooperation expectations are creating confusion as well. DAG Monaco further justified

5. *Id.*
6. Lisa Monaco, Deputy Attorney General, U.S. Dep't of Justice, Keynote Address at ABA's 36th National Institute on White Collar Crime (Oct. 28, 2021), available here: https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute. The restored DOJ policy on cooperation is a nod to the September 2015 Memorandum from then-Deputy Attorney General Sally Q. Yates titled "Individual Accountability for Corporate Wrongdoing" (the Yates Memorandum), where DOJ required companies seeking credit or leniency for cooperation to provide "all relevant facts about the individuals involved in corporate misconduct." Memorandum from Sally Q. Yates, Deputy Attorney General, U.S. Dep't of Justice, to All United States Attorneys (Sep. 9, 2015), available at https://www.justice.gov/archives/dag/file/769036/download.
7. Justice Manual, 4-4.112.

the policy shift by noting that "[t]he department's investigative team is often better situated than company counsel to determine the relevance and culpability of individuals involved in misconduct." While that may be true in certain situations, it does suddenly expand the scope of disclosures to include those employees who were merely "involved" in but were not "responsible" for the misconduct, which may put a number of potentially innocent or non-culpable – from a legal perspective – employees in the DOJ's crosshairs with marginal benefit to the investigation.

Strategic considerations of cooperation in the Biden Era

The changes announced by DAG Monaco revert back to the spirit of the Yates Memo and its focus on individual responsibility and accountability. It also removes some of the discretion companies previously had to determine who was substantially involved in wrongdoing. Given the new heightened standards for receiving DOJ cooperation credit, companies may want to recalibrate how they make decisions about disclosures and cooperation.

In making that calculus, it is helpful to consider what credit is potentially available for cooperation. The DOJ has always been somewhat opaque about this, but its view is that civil fraud cases are about returning money lost to the government – to compensate the government for its damages. Consistent with this view, the Justice Manual states that "[t]he maximum credit that a defendant may earn may not exceed an amount that would result in the government receiving less than full compensation for the losses caused by the defendant's misconduct (including the government's damages,[8] lost interest, costs of investigation, and relator share)." Those amounts are referred to as "single damages," which are often themselves significant and contested. But the FCA authorizes damages up to treble the amount of single damages alongside significant penalties for each false claim filed, and DOJ typically settles FCA cases for "double damages" even where cooperation is absent. Because the Justice Manual prevents cooperation credit from reducing the single damages amount, the incentive under DOJ policy for a company to cooperate is limited to reducing the damages multiplier used to arrive at an appropriate settlement figure and the per claim penalties. This raises the question of whether a defendant who earns cooperation credit actually benefits significantly compared to defendants who settle FCA claims without a cooperation credit.

8. As Jamie Yavelberg, the Director of the Civil Division Fraud Section, stated, "a credit will earn you a reduction, but the government is not going to take less than its losses; the government needs to be made whole." Jamie Yavelberg, Director, Fraud Section, Civil Division, U.S. Dep't of Justice, Keynote Address at the Twenty-Second PCF Virtual Pharmaceuticals and Medical Device Ethics & Compliance Congress and Best Practices Forum (Nov. 3, 2021).

Another consideration in FCA cases is that the settlement value for the government should reflect its own litigation risk in any given case. Depending on the strength of the government's case, the settlement value of an FCA claim could be at single damages – even without application of a cooperation credit. Where that is the case, cooperation credit may be of little value to a defendant. In fact, there is a risk that a defendant's cooperation lowers the government's litigation risk and therefore raises the settlement value in a way that could fully off-set any cooperation credit in some cases.

On the other hand, there can be intangible and non-monetary value in self-disclosure and cooperation. Cooperation can give companies influence or a voice in the course of the investigation and potential settlement, which could lead to a more favorable and earlier resolution of any claim. Likewise, true cooperation can lend more credibility to advocacy presentations or papers provided to DOJ and engender trust in the agencies tasked with oversight of the company, such as the Centers for Medicare and Medicaid (CMS) or the U.S. Dep't of Health and Human Services-Office of Inspector General (HHS-OIG).

Although the recent change in policy announced by DAG Monaco represents a departure from the more flexible approach of identification of individuals for purposes of cooperation, the monetary and intangible benefits to voluntary self-disclosure and cooperation in most cases likely remain unchanged. In some investigations, however, the strategic considerations underpinning the decision to voluntarily self-disclose and fully cooperate will require careful consideration in light of what a company may have to provide to meet the new stringent cooperation standard.

Anthony E. Fuller
Partner | Boston
+1 617 371 1032
anthony.fuller@hoganlovells.com

David I. Sharfstein
Partner | Washington, D.C., Baltimore
+1 202 637 5739 (Washington, D.C.)
+1 410 659 2721 (Baltimore)
david.sharfstein@hoganlovells.com

Looking ahead

The Biden Administration has made it clear that deterring corruption and fraud through aggressive enforcement – including the use of the False Claims Act – is a priority. With its leadership team beginning to take form, the Department of Justice (DOJ) is ready to take action. Although the pandemic may again slow some investigations and trials in 2022, we expect the pace of enforcement to pick-up on the whole. Specific FCA enforcement priorities continue to include pandemic-related fraud, fraud related to opioids, and conduct targeting seniors. In addition, DOJ's Civil Cyber Fraud Initiative underscores DOJ's commitment to using the FCA in new ways to reinforce cyber security obligations of government contractors and subcontractors and root out fraud. And, as in years past, businesses operating in the health care industry sector are under intense FCA scrutiny from the government and from would-be FCA whistleblowers. DOJ has indicated it is particularly focused on fraud related to telehealth and to the acquisition and implementation of electronic health records systems. The following emerging trends warrant close scrutiny in 2022 and appear to represent another active year of FCA enforcement.

An increase in telehealth and continued transition to electronic health records are likely to draw FCA scrutiny

The use of telehealth services has skyrocketed during the COVID-19 pandemic; we expect a significant portion of this expansion to endure. A number of recent FCA cases have scrutinized the practices of telemedicine companies and healthcare providers who utilize telehealth, and we expect this to continue. Allegations of fraud have recently related to orders for durable medical equipment, diagnostic tests, and compound medicines that aren't supported by sufficient patient diagnostic interaction. While similar cases may be on the horizon, new or novel FCA theories relating to telehealth services may also emerge. New regulations aiming to narrow opportunities for fraud in telehealth may also be forthcoming. Telemedicine companies and providers who utilize telehealth should therefore evaluate their compliance programs to ensure the length of patient diagnostic interactions are accurately documented in 2022 and closely monitor regulatory changes on the horizon. Although the vast majority of health care providers have already transitioned to electronic health records (EHR), we expect to see continued FCA enforcement activity in this area. EHR companies should confirm that their products are compliant with the latest requirements for the government incentive programs, and health care providers should ensure that their EHR software is

properly certified through the ONC Health IT Certification Program, publicly available at https://chpl.healthit.gov/#/resources/overview, and has previously maintained successful reliable outcomes.

DOJ's Civil Cyber-Fraud Initiative could have broad implications

In recent years we have seen that failures to comply with contractual and regulatory requirements relating to cybersecurity is a burgeoning area of FCA risk for government contractors and grant recipients. DOJ's recently-announced Civil Cyber-Fraud Initiative underscores this risk. This initiative seeks to organize and prioritize DOJ's efforts in this regard, and the initiative expressly aims to secure FCA recoveries to reimburse the government and taxpayers for losses incurred "when companies fail to satisfy their cybersecurity obligations." With this new initiative in place, we expect DOJ may be more prone to intervene in cases where whistleblowers make such allegations of noncompliance. The government's increased interest in aggressively enforcing compliance with cybersecurity requirements may also incentivize company insiders to examine their companies' cybersecurity obligations and practices and file FCA actions when they find possible compliance failures. The initiative may also draw government scrutiny not just from DOJ, but also from inspectors general at numerous government agencies who could in turn refer cases to DOJ. This initiative will likely result in a flurry of activity in 2022.

Noteworthy case law developments and DOJ policy changes

In addition to the above enforcement trends, several developing areas of case law and changes in DOJ enforcement policy will shape FCA litigation in 2022.

First, developments in the courts, and potentially in Congress, relating to the materiality requirement of the FCA could prove important this year. A key issue is under what circumstances – if any – conclusions about materiality can be reached in the early stage of litigation. Courts have recently declined to find any single fact dispositive with regard to materiality and instead taken a "holistic" view of the circumstances of each case, including government action or inaction despite knowledge of alleged misconduct. As a result, defendants have had less success challenging FCA claims on grounds of materiality at the motion to dismiss stage or even, in some cases, at summary judgment. We will be watching to see if this trend continues.

We will also be watching to see if additional courts consider the degree to which a defendant's assertion that its actions comported with an objectively reasonable interpretation of an ambiguous regulation prevents a finding of "knowing" misconduct,

which is required for an FCA violation. Key unanswered questions about an FCA defense premised on this principle include: (1) whether the asserted objectively reasonable interpretation of the regulation must also have been subjectively held by the defendant at the time the claim was submitted; (2) who bears the burden of proof; (3) what types of evidence show that a defendant held an objectively reasonable belief at a particular point in time; and (4) whether invoking the safe harbor triggers a waiver of the attorney-client privilege.

There is also continued disagreement in the courts about the standard of review for the DOJ's use of its power to dismiss declined qui tam suits under 31 U.S.C. § 3730(c)(2)(A). These motions are, and always have been, rare. Nonetheless, the lack of consensus about the legal standards applicable to these motions will impact some litigants who will have to continue – absent Congressional action – to maneuver through a deepening split among the circuits in the coming year.

Finally, DOJ's recent announcement that it has restored prior guidance requiring that, to be eligible for cooperation credit, companies must provide the DOJ with all non-privileged information about individuals involved in or responsible for the misconduct at issue in a case is certain to shape DOJ investigations and settlements in 2022. This is a departure from the more flexible, recent approach that allowed companies to benefit from a full cooperation credit if they met other requirements and identified only those individuals "substantially involved in or responsible for the misconduct." We will be watching to see how this renewed focus on individuals within companies will shape the course of investigations and FCA settlements in the year to come.

Staying on top of these and other potential developments in FCA enforcement will be critical for businesses moving forward. The FCA practice at Hogan Lovells stands ready to help you with our market-leading lawyers.

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
Sao Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.

*Our associated offices
Legal Services Centre: Berlin

www.hoganlovells.com