THE INTERNATIONAL ACADEMY
OF FINANCIAL CRIME LITIGATORS

Bulletin

of The International Academy of Financial Crime Litigators

ISSUE 1 | SUMMER 2023

Bulletin of The International Academy of Financial Crime Litigators

Paris, France

Editor: Jonathan S. Sack

Editorial Board/Publishers: Stéphane Bonifassi, Lincoln Caylor and Elizabeth Ortega

Publication/Art Director: ECO Strategic Communications

The Bulletin appears twice a year and is available free of charge.

Current and back issues are available online at:
https://financialcrimelitigators.org/publications/

To sign up for a subscription or to report an address change please send an email to contact@financialcrimelitigators.org.

For editorial comments or inquiries, please contact the editor at jsack@maglaw.com or at the address below.

For further information about The Academy, please visit our website www.financialcrimelitigators.org.

For general inquiries, please send an email to contact@financialcrimelitigators.org.

Contents

ISSUE 1 | SUMMER 2023

04 LETTER FROM THE EDITOR

WELCOME

to the first issue of The Bulletin of The International Academy of Financial Crime Litigators.

05 THE LEAD

The Risks of "Too Much" Entanglement with the Government When Conducting Internal Investigations: ***Benjamin Gruenstein & Rebecca Schindel***

17 **TRANSPARENCY**

The UK'S Economic Crime and Corporate Transparency Bill: ***Jeremy Horder & Gabriele Watts***

26 **CRYPTO**

Reining in Cryptocurrencies: Has the Horse Already Bolted? ***Keith Oliver & Caroline Timoney***

35 **FIN CRIME**

ESG and Financial Crime - a European Perspective: ***David S. Schreuders***

44 **CLAWBACKS**

Compensation Clawbacks: Domestic and International Considerations of DOJ Pilot Program: ***Diana K. Lloyd & Meg E. Ziegler***

51 **FORFEITURE**

A Swiss–Peruvian Asset Recovery Case Boosts Prospects for Non-Conviction Based Forfeiture in the Fight Against Transnational Corruption and Money Laundering: ***Oscar Solórzano & Gretta Fenner***

58 **THE INTERNATIONAL ACADEMY OF FINANCIAL CRIME LITIGATORS**

FOUNDERS

Letter FROM THE EDITOR

Welcome to the first issue of the Bulletin of The International Academy of Financial Crime Litigators. As the editor, I am honored to be given the opportunity to make the Bulletin The Academy's latest vehicle for transmitting the work of Academy Fellows and contributing to the legal profession. The Academy has in-person conferences in Europe and the United States, ad hoc virtual get-togethers, and many informal exchanges among colleagues. Now comes the Bulletin to take the dialogue a step further. The Academy's mission is to join theory and practice. The Bulletin is our opportunity to deepen our knowledge as practitioners and raise awareness of important issues in the legal profession.

This first issue of the Bulletin achieves these goals admirably. The articles highlight the global and transnational implications of developments in the realm of financial crime. We have two articles about developments in U.S. Department of Justice (DOJ) policies that affect companies subject to the broad reach of the DOJ.

Ben Gruenstein* and Rebecca Schindel address thorny questions that come into play when a company decides to cooperate with a DOJ investigation. While such cooperation has become common, and has distinct benefits, it is not without peril for both the company and its counsel. As Ben explains, "guardrails" around the process are needed to make sure that counsel serves the interest of the corporate client, and the rights of employees and defendants are respected.

Diana Lloyd* and Meg Ziegler discuss a new DOJ pilot program to give companies incentives to "claw back" compensation from employees found to have engaged in wrongdoing. Diana places the pilot program in the context of earlier government efforts to encourage clawbacks and asks important questions about how such efforts might work in practice.

We also have several articles focusing on developments in the UK and the Continent.

Jeremy Horder and Gabriele Watts* discuss the UK's new Economic Crime and Corporate Transparency Bill and tease out issues and tensions in the proposal, which, if adopted, would make significant changes in the scope of corporate criminal liability and create a new offense of "failing to prevent" certain offenses.

Keith Oliver* and Caroline Timoney address the burgeoning problem of fraud in the world of cryptocurrency and describe new and proposed regulatory frameworks around the world. They consider the trenchant question of whether, by the time the regulators act, the horse has already left the barn.

David Schreuders* looks at an issue of growing importance in the law and policy realm--Environmental, Social and Governance (ESG) objectives—and explores how criminal enforcement in the European Union is increasingly becoming a tool to achieve ESG goals.

Oscar Solorzano and **Gretta Fenner*** analyze a recent decision of the Swiss Federal Supreme Court which cleared the way for returning funds tied to corruption to Peru. The important decision highlights the use of forfeiture laws to recover illicit assets even in the absence of a criminal conviction. They explain how the case may bolster the fight against global corruption.

I wish to close on a personal note. All of us have come to the law as a career and vocation for personal reasons. However, as Fellows of The Academy, we share bedrock principles — among them, practicing law at the highest ethical and professional level, and zealously pursuing justice for our clients. I would be deeply gratified if this Bulletin becomes one more way we contribute to this noble enterprise.

**** Fellows of The Academy***

I hope you enjoy this inaugural issue of

The Academy Bulletin.

Jonathan S. Sack* | *Editor*

The Lead

The Risks of "Too Much" Entanglement with the Government When Conducting Internal Investigations

BENJAMIN GRUENSTEIN

REBECCA SCHINDEL

Introduction

The U.S. Department of Justice's policy on corporate criminal enforcement, refreshed on October 28, 2021 and further refined on September 15, 2022, places renewed emphasis on individual accountability. In a break from Trump-era policy, the DOJ now requires corporations hoping to receive *any* cooperation credit in criminal investigations to "disclose to the Department all relevant, non-privileged facts about individual misconduct," and to do so "swiftly and without delay." Lisa Monaco, Deputy Attorney General, U.S. Department of Justice, Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group at 3 (Sept. 15, 2022) [hereinafter, "Monaco Memo"]. As the latest guidance warns, "[c]ompanies that identify significant facts but delay their disclosure will place in jeopardy their eligibility for cooperation credit." *Id.*

This policy places company counsel that are conducting internal investigations in a difficult position. Companies seeking to limit or avoid liability in a DOJ probe have strong incentives to coordinate closely with the DOJ in identifying and investigating potential wrongdoers. Too much cooperation, however, risks undermining the ultimate success of any DOJ action and raises significant ethical and legal concerns for company counsel. This article addresses some of those potential pitfalls.

OVERVIEW OF DOJ'S CORPORATE ENFORCEMENT POLICY

In 2015, the U.S. Department of Justice articulated a policy on corporate enforcement that focused on identifying and prosecuting individual wrongdoers. That policy, introduced by then-Deputy Attorney General Sally Yates, emphasized the DOJ's efforts to hold individual wrongdoers accountable for corporate wrongdoing. To further that effort, the Yates Memo announced an "all-or-nothing" approach to corporate cooperation. If companies wished to receive any cooperation credit from the DOJ, they were required to identify "all individuals involved in or responsible for the misconduct at issue, regardless of their position, status or seniority." Sally Quillian Yates, Deputy Attorney General, U.S. Department of Justice, Individual

Accountability for Corporate Wrongdoing at 3 (Sept. 9, 2015) [hereinafter, "Yates Memo"]. The Yates Memo also made clear that the DOJ would not "release culpable individuals" from liability when resolving a matter with a corporation "absent extraordinary circumstances or approved departmental policy," and any attempt to resolve matters with a corporation should be accompanied by a "clear plan to resolve related individual cases." *Id.* at 2.

The DOJ changed tack under the Trump Administration and walked back the Yates Memo's "all-or-nothing" approach to corporate cooperation credit. In November 2018, then-Deputy Attorney General Rod Rosenstein announced that corporations could receive cooperation credit in criminal investigations if the corporation "identif[ied] every individual who was substantially involved in or responsible for the criminal conduct"—*i.e.*, not all involved individuals, as the Yates Memo had required. Rod J. Rosenstein, Deputy Attorney General, U.S. Department of Justice, Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act, Oxhon Hill, MD (Nov. 29, 2018). In fact, DAG Rosenstein specifically advised that investigations "should not be delayed merely to collect information about individuals whose involvement was not substantial, and who are not likely to be prosecuted," and he encouraged companies seeking cooperation credit to have "full and frank discussions with prosecutors about how to gather the relevant facts." *Id.* In civil investigations, DOJ rolled back the "all-or-nothing" policy even further, noting that corporations could receive cooperation credit (albeit not full credit) if they identified "all wrongdoing by senior officials, including members of senior management or the board of directors," even if they failed to identify all individuals who were substantially involved in or responsible for the misconduct. *Id.*

Then, in October 2021, the Deputy Attorney General under President Biden, Lisa Monaco, announced yet another set of changes to the DOJ's corporate enforcement policy. These revisions, which Monaco further refined in a speech and a memo released in September 2022, mark a clear return to the "all-or-nothing" policy set forth in the Yates Memo. A company seeking any cooperation credit "must disclose to the Department all relevant, non-privileged facts about individual misconduct." Monaco Memo at 3. Moreover, such disclosures must be made "swiftly and without delay," and companies must prioritize turning over evidence "that is most relevant for assessing individual culpability," including "information and communications

associated with relevant individuals during the period of misconduct." *Id.* The penalty for failing to cooperate fully and swiftly is steep: "undue or intentional delay in producing information or documents—particularly those that show individual culpability—will result in the reduction or denial of cooperation credit." Lisa O. Monaco, Deputy Attorney General, U.S. Department of Justice, Remarks on Corporate Criminal Enforcement, New York, NY (Sept. 15, 2022). As DAG Monaco put it in her September 2022 remarks, "[i]f a cooperating company discovers hot documents or evidence, its first reaction should be to notify prosecutors." *Id.* To further disincentivize delay, the Monaco Memo instructed prosecutors to complete investigations into individuals and seek any warranted criminal charges prior to or simultaneously with the entry of a resolution against the corporation. Monaco Memo at 3.

In addition to penalizing delay, DAG Monaco's policy also introduced several "carrots" to incentivize cooperation. Most notably, in her September 2022 speech, DAG Monaco announced a new policy whereby "every Department component that prosecutes corporate crime will have a program that incentivizes voluntary self-disclosure." If any component lacked a formal, documented policy, it would be required to draft one. One common principle would govern all components' policies: if a company voluntarily discloses, cooperates and remediates, then the DOJ will not seek a guilty plea absent aggravating factors. Thus, as DAG Monaco explained, "the clearest path for a company to avoid a guilty plea or an indictment is voluntary self-disclosure."

In short, DAG's Monaco's policy changes reinforced the DOJ's emphasis on individual culpability and exerted greater pressure on corporations to cooperate quickly and fully when they encounter evidence of potential wrongdoing.

POTENTIAL PITFALLS OF "TOO MUCH" COOPERATION

The DOJ's emphasis on individual accountability creates strong incentives for companies to align themselves with the government during a criminal investigation, as rooting out individual wrongdoers will help secure cooperation credit and potentially stave off a guilty plea or indictment. However, unless certain guardrails are in place, such alignment has the potential to raise significant constitutional and ethical concerns.

Constitutional issues may arise, for instance, if the government presses the company to interfere with employees' Fifth Amendment right against self-incrimination or Sixth Amendment right to counsel. Perhaps the most notorious example of government overreach is *United States v. Stein*, 435 F. Supp. 2d 330 (S.D.N.Y. 2006), *aff'd*, 541 F.3d 130 (2d Cir. 2008). In *Stein*, KPMG was the target of a government investigation that implicated senior partners, including the deputy chair and chief operating officer of the firm, Jeffrey Stein. *Stein*, 435 F. Supp. 2d at 339. KPMG initially agreed to pay for the partners' legal expenses in any suits related to the alleged misconduct. *Id.* DOJ attorneys, however, conveyed to KPMG "that payment of legal fees by KPMG, beyond any that it might legally be obligated to pay, could well count against KPMG in the government's decision whether to indict the firm." *Id.* at 344. The DOJ issued such warnings in accordance with the then-controlling "Thompson Memorandum," which required prosecutors to consider, among other things, whether a company elected to pay legal fees for its employees and whether a company continued to employ or support employees who asserted their Fifth Amendment rights when deciding whether to indict a corporate entity. Larry D. Thompson, Deputy Attorney General, U.S. Department of Justice, Principles of Federal Prosecution of Business Organizations at 7-8 (Jan. 20, 2003). In light of this policy, KPMG decided that it would pay legal fees only for partners or employees who agreed to cooperate fully with the government and to cut off payment of legal fees for anyone who was indicted. *Stein*, 435 F. Supp. 2d at 345-46.

Stein and a number of other KPMG personnel were ultimately indicted and, "[t]rue to its word, KPMG cut off payments to the defendants of legal fees and expenses." *Id.* at 350. Stein and his co-defendants challenged the government's successful campaign to persuade KPMG not to pay their legal fees and expenses as a violation of their constitutional rights. The court agreed, holding that the government's conduct had violated Stein and his co-defendants' Fifth Amendment right to a fair criminal process and the defendants' Sixth Amendment right to counsel. *Id.* at 382. In so ruling, the court rejected the government's claim that the United States had neither "coerced" nor "bullied" KPMG into cutting off payment for the individual defendants' legal expenses, observing that such an assertion could "be justified only by tortured definitions of those terms." *Id.* at 381. Following *Stein*, the DOJ issued new guidance (the so-called "McNulty Memorandum"), which prohibited prosecutors from considering whether a

corporation paid its employees' legal fees in connection with a government investigation, except where "the totality of the circumstances show that [such indemnification] was intended to impede a criminal investigation." Paul J. McNulty, Deputy Attorney General, U.S. Department of Justice, Principles of Federal Prosecution of Business Organizations at 11 & n.3 (Dec. 12, 2006).

Although *Stein* and the McNulty Memorandum curbed DOJ's efforts to influence companies in the payment of employees' legal expenses, more recent examples of close coordination between the government and companies have continued to raise constitutional concerns. For instance, in *United States v. Connolly*, No. 16-cr-0370, 2019 WL 2120523 (S.D.N.Y. May 2, 2019), then-Chief Judge McMahon of the U.S. District Court for the Southern District of New York, criticized the DOJ for "outsourc[ing] its investigation" of LIBOR manipulation to the target of the investigation, Deutsche Bank, and its outside counsel. *Id.* at *1. When Deutsche Bank first learned that it was under investigation, it "immediately decided that it would go all-in with cooperation." *Id.* at *2. The government instructed the bank's counsel on, among other things, whom to interview, when to interview them and how to conduct the interviews. Bank counsel interacted with the government on "hundreds if not thousands of occasions," and for the final 14 months of the banks' internal investigation, "counsel held joint 'weekly update calls' to provide the Government with the latest developments and afford it an opportunity to 'make new requests.'" *Id.* at *7. Moreover, rather than "simply respond[ing] to Government document requests by producing responsive documents for the Government's review," the bank also "flagged 'notable' . . . evidence or information that [it] believed would be of particular interest' to the Government," provided the government with "real time updates about facts gleaned from employee interviews" and made sure to ask government for "permission" to re-interview one of its own employees—Gavin Black—as part of its internal investigation. *Id.* at *6-7.

During the five years that Deutsche Bank was conducting its internal investigation, there was no evidence that the DOJ was conducting a "substantive parallel investigation" of its own. *Id.* at *9. Rather, the court surmised, the lack of evidence of any "independent investigative activities" indicated that the DOJ simply "g[a]ve direction" to Deutsche Bank and its counsel, took "the results of their labor (which appears to have been fully disclosed to Government lawyers), and save[d] itself the trouble of doing its own work." *Id.*

Ultimately, the investigation led to criminal charges against three Deutsche Bank employees, including Gavin Black, who later challenged his indictment as unconstitutional. He argued that his interview statements to Deutsche Bank's outside counsel were "fairly attributable" to the government because of the degree to which the government directed Deutsche Bank's investigation, and that those statements were "compelled" and the "product of coercion." *Id.* at *10. As a result, he claimed that his indictment ought to be dismissed under *United States v. Kastigar*, 406 U.S. 441 (1972), which held that "[a]ny use, direct or indirect, of a defendant's compelled statements is unconstitutional under the Fifth Amendment's self-incrimination clause." *Id.* at *15; *see also Kastigar*, 406 U.S. at 453.

The court agreed that the Deutsche Bank's investigation was "fairly attributable" to the government in that the DOJ effectively "directed Deutsche Bank to investigate Gavin Black on its behalf." *Connolly*, 2019 WL 2120523 at *11. There was also "no question in the Court's mind that Black was compelled, upon pain of losing his job, to sit for at least three, probably four, interviews" with the bank's counsel. *Id.* Nevertheless, the court concluded that there was no *Kastigar* violation because the government did not use Black's statements at trial, before the grand jury or during its investigation. *Id.* at *21-22.

The *Connolly* decision highlights the significant constitutional risks that arise when companies and company counsel are perceived to serve as an arm of the government when investigating potential wrongdoing. Indeed, shortly after *Connolly* was decided and likely in response to the decision, the DOJ modified guidance in its FCPA Corporate Enforcement Policy to make clear that, "[a]lthough the Department may, where appropriate, request that a company refrain from taking a specific action for a limited period of time for de-confliction purposes, the Department will not take any steps to affirmatively direct a company's internal investigation efforts." Justice Manual, Principles of Federal Prosecution of Business Organizations, FCPA Corporate Enforcement Policy, 9-47.120 n.2 (updated Nov. 2019). This update reflects an effort to set appropriate boundaries between the DOJ and company counsel when a company opts to cooperate. But even still, the line between undue entanglement and extensive cooperation is not always clear. It is made all the murkier by DAG Monaco's recent guidance, including, for instance, her insistence in her September 2022 remarks that a company's "first reaction" upon learning of "hot documents or evidence . . . should be to notify prosecutors"—presumably even while an internal investigation is still ongoing.

Even apart from its constitutional implications, *Connolly* underscores the tricky ethical and legal considerations that come into play when companies and their counsel are considering voluntary self-disclosure or cooperating in a DOJ probe. On the one hand, extensive cooperation is often in a company's best interests. Indeed, the court in *Connolly* noted that Deutsche Bank's strategy of extensive cooperation was a "conspicuous success" for the bank. Even though Deutsche Bank had not voluntarily self-disclosed, it avoided both a guilty plea and an indictment and was able to sign a Deferred Prosecution Agreement with the DOJ, under which it paid a $775 million fine, agreed to continue cooperating in the government's ongoing investigation and retain a corporate monitor for three years. *Connolly*, 2019 WL 2120523, at *8. Had Deutsche Bank been forced to plead guilty, by contrast, its operating subsidiaries would have lost "key licenses and authorizations in the United States" and it "would have lost business in virtually all aspects of its operations." *Id.*

At the same time, the incentive to cooperate necessarily creates a tension between the company and its employees, as the company wants to encourage its employees to cooperate with its own internal investigation to the greatest extent, while reserving the right to identify those same cooperators to the DOJ as wrongdoers if any misconduct comes to light. Companies and company counsel must therefore take care to abide by their ethical obligations to be honest and transparent in their dealings with employees, even as they are incentivized to disclose as much as possible as early as possible in an investigation. The standard *Upjohn* warnings issued to employees being interviewed during the course of an internal investigation—*i.e.*, warnings from counsel conducting the interview that they represent the company and not the employee, and that any privileged information gathered during the interview could be shared with third parties, including the government, at the company's discretion—may not be sufficient in all cases.

The commentary to Rule 1.13 of the New York Rules Professional Conduct, for instance, advises that if company counsel thinks a conflict *may* develop between the company and an employee, counsel should specifically warn the employee of the potential conflict and note that the employee may wish to obtain independent representation. Although this commentary has not been adopted by the Appellate Division of the New York Supreme Court and therefore is not binding, it is nonetheless telling about the extent to

which company counsel are expected to protect and respect the interests of individual employees—including potential wrongdoers.

Absent full transparency in communications between company counsel and employees, there is a real risk that the scope and nature of counsel's representation will be misunderstood or misconstrued. Indeed, there is currently a motion pending in *United States v. Gregoire Tourant*, a case in the Southern District of New York, arguing that the indictment against the defendant (Gregoire Tourant, a former Allianz employee) should be dismissed because it was secured based on privileged communications between Tourant and his counsel, which the government allegedly "induced" the company counsel to reveal. In *Tourant*, Allianz's counsel initially represented both the company and Tourant. Tourant alleges, however, that his attorneys "ultimately concluded that the Government's investigation presented an existential threat to Allianz," and, "[i]n an effort to stave off a possible indictment against Allianz, counsel made the choice to misuse their attorney-client relationship with Mr. Tourant to obtain additional statements from him about the subject matter of the case, which they subsequently disclosed to the Government." Mem. of Law ISO Defendant George Tourant's Mot. to Dismiss the Indictment, or, In the Alternative, for a Hearing at 2, *United States v. George Tourant*, No. 1:22-cv-00276-LTS (S.D.N.Y. Jan. 30, 2023), ECF No. 54. According to Tourant, "[t]he Government not only encouraged and permitted [counsel's] actual betrayal of its former client, but [counsel's] actions are additionally attributable to the Government due to the coercive pressure placed on Allianz by the Government's corporate cooperation policies." *Id.* at 26. The motion has not been decided, and the government strenuously denies that it received any privileged information from Tourant's former counsel or that there is any basis to "attribute any action by Allianz or its law firms to the Government." The Government's Response in Opposition to Defendant's Mot. to Dismiss the Indictment and to Compel at 16, *United States v. George Tourant*, No. 1:22-cv-00276-LTS (S.D.N.Y. Feb. 17, 2023), ECF No. 61. Whatever way this motion is ultimately decided, it underscores the importance of communicating clearly with employees during the course of internal and government investigations and carefully demarcating the bounds of any attorney-client relationship.

There may be other legal and business implications, too, from excessive alignment between company counsel and the government. For instance, certain countries have implemented "blocking statutes," which aim to limit the transfer of sensitive information outside the countries' borders. France's blocking statute, for example, prohibits any person from requesting, searching for or communicating "documents or information of an economic, commercial, industrial, financial or technical nature" for use as evidence in a "foreign judicial or administrative procedure," unless done pursuant to an international treaty or agreement to which France is a party. Ela Barda & Thomas Rouhette, "The French Blocking Statute and Cross-Border Discovery," IADC (Feb. 7, 2020). Documents and information gathered as part of a purely internal investigation would not run afoul of this statute because such material would not be collected in connection with a "judicial or administrative procedure." But as Academy fellow Frederick Davis has written, if an internal investigation is unduly directed or influenced by the DOJ—as the court concluded had occurred in *Connolly*—then a French judge may decide that the U.S. lawyers conducting the investigation have violated French law. Frederick T. Davis, United States v. Conolly *and the Risk That 'Outsourced' Criminal Investigations Might Violate Foreign Blocking Statutes*, New York U. Program on Corporate Compliance & Enforcement.

There is also the risk that helping the government target a suspected wrongdoer will backfire on the company if the government is wrong or lacks enough evidence to secure a conviction. In *United States v. Bogucki*, No. 18-cr-021, 2019 WL 1024959 (N.D. Cal. Mar. 4, 2019), for instance, Judge Charles Breyer of the Northern District of California dismissed the government's criminal fraud case against a former Barclays trader after the government rested and before the case went to the jury—the first time Judge Breyer had issued such a ruling in his more than 20 years on the bench. Aruna Viswanatha, *Flaws Emerge in Justice Department Strategy for Prosecuting Wall Street*, Wall Street Journal (July 5, 2021).

In *Bogucki*, the DOJ alleged that the former head of Barclays' over-the-counter foreign exchange trading desk had committed fraud by misusing a corporate client's, HP Inc.'s, information to benefit the bank at HP's expense. *Id.* The DOJ learned about Bogucki's alleged misconduct from Barclays directly, which was required, as part of a plea deal it had previously signed in a separate case, to disclose to the government signs of potential fraud that it might encounter.

When Barclays found audio recordings relevant to the deal in question "that its lawyers considered troubling," Barclays retained outside counsel to conduct an internal review. *Id.* Those lawyers briefed the DOJ about their findings and notified the DOJ that they intended to interview Bogucki. *Id.* The outside lawyers conducted the interview in July 2016, and Bogucki was placed on paid leave in November 2016 while Barclays and its lawyers "continued to hand evidence to the DOJ." *Id.* Bogucki was indicted by a federal grand jury on wire fraud and other charges in January 2018. At trial, the government was required to prove that Bogucki had made materially false statements to HP as part of a scheme to defraud. The court found that Bogucki had not made any "false statements or material omissions that were capable of influencing a person in . . . HP's position to part with money or property," and that the government was instead "pursu[ing] a criminal prosecution on the basis of conduct that violated no clear rule or regulation, was not prohibited by the agreements between the parties, and indeed was consistent with the parties' understanding of the arms-length relationship in which they operated." *Bogucki*, 2019 WL 1024959 at *6-7. As a result, the court granted Bogucki's motion to dismiss the indictment as to all counts. *Id.* at *7.

After his victory in court, Bogucki sued Barclays for his suspension and lost earnings, and the bank settled the case for an undisclosed sum in May 2020. Viswanatha, *supra*. Notably, Barclays had suspended Bogucki following his interview with outside counsel even though Barclays had told DOJ prosecutors that "the trading didn't look like fraud and that they would have trouble proving their theory at trial." *Id.* Though the details of Bogucki's settlement with Barclays are not public, it seems plausible that the bank's decision to discipline him in accordance with the government's theory of liability factored into the settlement terms. The risk of lawsuits from disgruntled and vindicated employees is also something companies must consider when deciding how and when to cooperate with government probes.

All together, these risks highlight the tight rope companies and company counsel must walk when they encounter potential wrongdoing in their ranks. Although it is often in a company's best interest to cooperate extensively with the government, both the company and company counsel must take care to maintain an appropriate professional distance from the government and to conduct their own internal investigation without undue direction from the government. At the same time, to comport with their legal and ethical

obligations, company leadership and company counsel must be direct, transparent and fair in their dealings with employees. Only by maintaining these appropriate, professional dealings can companies and their counsel avoid the constitutional, ethical and business pitfalls that arise from "too much" cooperation with the government in times of corporate distress.

AUTHORS

Benjamin Gruenstein

Fellow Benjamin Gruenstein is a partner in Cravath's litigation department in New York. He is a member of the firm's investigations and regulatory enforcement practice.

Rebecca Schindel

Rebecca J. Schindel is of counsel in Cravath's litigation department in New York. Her practice focuses on antitrust and general corporate litigation.

Transparency

The UK'S Economic Crime and Corporate Transparency Bill

JEREMY HORDER

GABRIELE WATTS

Introduction

On January 25, 2023, led by former Secretary of State for Justice Sir Robert Buckland, MPs tabled crucial amendments to the UK's Economic Crime and Corporate Transparency Bill 2023, affecting the law of corporate crime. If accepted and enacted, these amendments would have profound implications for the shape and direction of corporate criminal law in the UK.

Clause 5 of the amendments seeks to replace or substantially modify the current governing doctrine of corporate liability, in so far as it applies to serious economic crimes. This doctrine is known as the "identification doctrine" (*Tesco v Nattrass* [1972] AC 153), which we will consider in the next section. Further, the amendments propose new offenses of 'failing to prevent' fraud, false accounting and money laundering (Clause 4), and propose an extension to the regime of individual corporate officer criminal liability (Clause 6). Clause 6 extends the regime of individual criminal liability to certain cases in which an officer was aware of a risk that their company might commit a failure-to-prevent offense contrary to clause 4. Clause 4 will be considered in section 3 below (limitations of space prevent any consideration of the detail of clause 6).

REPLACING THE 'IDENTIFICATION' DOCTRINE

Currently, if a company is to be convicted of a serious economic crime, that crime must have been committed by one or more persons who, in law, speak and act for (and hence, who can be identified with) the company itself. These persons are "those natural persons who by the memorandum and articles of association or as a result of action taken by the directors, or by the company in general meeting pursuant to the articles, are entrusted with the exercise of the powers of the company [*Tesco v Nattrass* [1972] AC 153, 199 to 200, Lord Diplock)."

If the crime is committed by someone in a subordinate (employee or agent) corporate capacity, even if that person exercises some managerial or supervisory functions, then the crime is not that of the company itself but of the individual in question (*Tesco v Nattrass* [1972] AC 153, 171, Lord Reid). While in a way perfectly intelligible, as an approach to corporate criminal responsibility, the identification doctrine has serious deficiencies, as a basis

for holding companies to account. It provides insufficient accountability in criminal law when, for example, regional or other very senior managers below board level have engaged in serious economic crime with the purpose of benefiting the company. In R *v Andrews Wetherfoil Ltd* ([1972] 1 WLR 118), for example, it was held that the manager of a company's housing division did not, when engaging in bribery, represent the company itself, and so the company was not criminally responsible in virtue of his actions. Similarly, if a subsidiary company engages in serious economic crime, the main company will not be criminally liable, even if it knew perfectly well what the subsidiary was doing. That is an embarrassment to a criminal justice system in which 79% of respondents to the Government's 2017 call for evidence on corporate criminal law reform considered that the current rules inhibit prosecutors from holding companies to account (https://www.transparency.org.uk/corporate-criminal-liability-law-commission-review-money-laundering-UK).

With what test do the amendments to the Bill propose to replace or modify the identification doctrine? The Clause 5 amendment will sweep away key elements of the doctrine, in so far as it applies to the crimes of fraud, false accounting, bribery, tax evasion and money laundering (economic crimes). Under Clause 5, a company will itself be liable for an economic crime, if such a crime is committed 'with the consent, connivance or neglect' of a 'senior manager' in the company. The first part of the proposed new clause 5 of the Bill reads as follows:

Clause 5—Identification doctrine—

1. A body corporate commits an offense of fraud, money laundering, false accounting, bribery and tax evasion where the offense is committed with the consent, connivance or neglect of a senior manager.

2. An individual is a "senior manager" of an entity if the individual—

a. plays a significant role in—

(i) the making of decisions about how the entity's relevant activities are to be managed or organised, or

(ii) the managing or organising of the entity's relevant activities, or

b. is the Chief Executive or Chief Financial Officer of the body corporate.

This proposal is drawn in part from the Australian Criminal Code, under which corporate fault may be found if and when, 'a high managerial agent of the body corporate intentionally, knowingly or recklessly engaged in the relevant conduct, *or expressly, tacitly or impliedly authorised or permitted the commission of the offence*.' The explicit specification of particular officers – the chief executive and the chief financial officer – as officers deemed to represent the company itself, is a proposal drawn from section 22 of the 2003 (as amended) Canadian Criminal Code. What should we make of the amended Clause 5?

Clause 5 widens the range of individuals whose conduct, decisions and state of mind will be treated as, in law, implicating the company. Anyone who 'plays a significant role' in 'the managing or organising of the entity's relevant activities' would count as such an individual. Quite clearly, for example, a store manager, or perhaps – in a flagship store - even such a person's (de facto) deputy, will count, even if such a person has no role whatsoever to play in overall corporate governance or in deciding the strategic direction of the company as a whole. Clause 5 is intended to make the attribution of criminal liability turn on proof of a link between the offending person and a person in authority within the company. In that way, Clause 5 is meant to avoid the introduction a scheme of straightforwardly vicarious corporate liability for the criminal acts of employees or agents, the kind of liability found in the United States.

Yet, the result is a curious half-way house. On the one hand, even if an employee commits a serious economic crime in order to benefit the company, that will not automatically lead to the company itself being criminally liable. On the other hand, such liability can be imposed on the company if that economic crime was committed with the consent, connivance or neglect of someone who, whilst they might have had some managerial authority, may be so remote from board level (or even regional manager-level) decision-making, that the imposition of liability on the company has strong elements of vicarious liability. Consequently, there is a risk of the proposed scheme of liability falling between two stools. The Clause 5 scheme makes companies themselves liable even when relatively low-level managers "go rogue" and allow economic crime to be committed by employees or agents on their watch. This is a notorious vice of vicarious liability models of corporate crime. Yet, the scheme also allows companies to escape liability if there was no

managerial fault, even if it turns out that they have benefitted from serious employee criminality over decades. Clause 5 thus fails to acknowledge that a key element of corporate fault may lie just as much in a failure adequately to manage and control (low-level) managers, as it does in a failure adequately to manage and control (mere) employees and agents. At the very least, then, clause 5 should have added to it a defense involving proof by the company that it had adequate or reasonable procedures in place to ensure that employees and agents were properly informed, supervised and controlled by their line managers, in relation to the prevention of economic crime.

Another key aspect of the Clause 5 proposal goes significantly further than either of its Australian or Canadian equivalents. Clause 5 permits criminal liability for fraud, false accounting, bribery or tax evasion, to be attributed to a company not only when the offence occurred with the "consent or connivance" of a senior company officer, but also when the offence occurred with the "neglect" of such an officer. From a prosecutor's point of view, this makes it much easier to secure evidence that will sustain a conviction of the company, in relation to crimes committed by employees or agents. That is because "neglect" may readily be inferred from (say) mere inaction on the part of a manager over a period of time. By contrast, other than in exceptional circumstances, proof of both "consent" and "connivance" on a manager's part must almost inevitably involve reliance on specific oral or written evidence of a manager's state of mind at a particular time. The latter may be much harder to prove. In principle, though, a combination of employee criminality and (adequately high-level) managerial neglect relating to that criminality, ought to be regarded as sufficient to fix a company with liability for the crime. The puzzle about this new form of liability comes in relation to the way in which it is meant to co-exist with existing and proposed offenses of failure-to-prevent economic crime. If the prosecution can establish direct corporate liability for a serious economic crime by showing that, due to neglect on the part of a (possibly quite low-level) manager, an employee or agent committed such a crime, why would the prosecution ever bother to charge the company with an offence of 'failure-to-prevent' that crime? Given that a defense of adequate or reasonable procedures is available to the company in the case of the latter (failure-to-prevent crime), but not in the case of the former (direct liability under clause 5), a prosecutorial choice to go for the former seems inevitable in almost every case.

AN OFFENCE OF FAILING TO PREVENT FRAUD

It is perhaps, inevitable that the UK will introduce an offense of corporate failure to prevent fraud. According to official statistics, in the year ending March 2022, there were no less than 4.4 million fraud offenses. Fraud losses in the UK stand at around £190 billion every year, with the private sector hit hardest, losing around £140 billion (the public sector may be losing more than £40 billion and individuals around £7 billion). Yet, in 2021, only 50,000 cases ended up being investigated by police and just 4,924 resulted in a charge in 2021-22. Will a failure-to-prevent fraud offense do something to change this picture?

The new clause 4 amendment proposes the following offence:

1. A relevant commercial organization ("C") is guilty of an offense under this section where—

- **a.** a person ("A") associated with C commits a fraud, false accounting or an act of money laundering, or aids and abets a fraud, false accounting or act of money laundering, intending—
  - (i) to confer a business advantage on C, or
  - (ii) to confer a benefit on a person to whom A provides services on behalf of C, and
- **b.** fails to prevent the activity set out in paragraph (a).

2. C does not commit an offence where C can prove that the conduct detailed in subsection (1)(a) was intended to cause harm to C.

3. It is a defence for C to prove that, at the relevant time, C had in place procedures that were reasonable in all the circumstances and which were designed to prevent persons associated with C from undertaking the conduct detailed in subsection (1)(a).

Clearly, this offense – which applies to false accounting and money laundering as well as to fraud -- is based on the template provided by the existing offenses of failure-to-prevent bribery and failure-to-prevent the facilitation of tax evasion. However, the clause 4 offence has much greater potential to substantially increase the costs of compliance for many businesses than its bribery/facilitation of tax evasion counterparts. The overwhelming majority of domestic firms face very small risks that their employees or agents will

commit bribery or facilitate tax evasion. So, significant costs in relation to compliance with these offences have been confined to a relatively restricted range of firms, perhaps especially (in the case of bribery) those trading internationally who were already under obligations to comply with the Foreign Corrupt Practices Act of 1977. By contrast, a broader failure-to-prevent economic crime offense, that covers fraud, false accounting and money laundering, affects almost every small business. Even in a two-person plumbing firm in Wimbledon, there is at least some risk that the sole employee will (say) be tempted to inflate costs incurred in billing customers, or to issue repeat invoices in the hope that the company will be paid more than once. That is not an objection to the introduction of the failure-to-prevent fraud offense, as such: far from it. However, there will be a much greater need in relation to this offense, than there was when the other failure-to-prevent offences were introduced, to ensure that the guidance issued in relation to the "reasonableness" of a firm's crime-prevention procedures provides a clear path to avoiding disproportionate burdens.

Having said that, clause 4 does avoid two significant risks of over-criminalization. First, the amended clause 4 is confined to economic crimes committed by "insiders" (employees; agents) that are aimed at third d parties ("outsiders") in order to benefit the company. It will not cover economic crimes aimed at enriching the employee/agent fraudster themselves at their own company's expense. That is an important restriction, because something like a third of company-related frauds are frauds committed by insiders to the detriment of their own company. More significantly, secondly, consider the question whether a failure-to-prevent fraud offence should cover cases in which a financial institution fails to prevent one of its customers being defrauded by a third party who persuades the customer to move money from an account with that institution. Half of all fraud cases now involve phishing, and in 32% of phishing cases, the fraudster pretends to be someone representing a financial institution (Office for National Statistics, 2022). So, it is legitimate to insist that financial institutions are doing their utmost to prevent such frauds (frauds commonly committed in their name), as these institutions are almost inevitably involved in the perpetration of the fraud, even if innocently and unwittingly. However, a failure-to-prevent fraud offense drafted so as, in principle, to cover such cases would involve a huge extension of the reach of corporate criminal law. The proposed new offense in the amended clause 4 does not go so far. As we have already indicated, clause 4 applies only to

economic crime perpetrated by persons, such as employees and agents, already associated with the commercial organization in question ("insiders"). It does not extend to a failure to prevent a fraud committed by an outside fraudster. That is the right approach. When victims have been fraudulently persuaded to move money out of their accounts, full reimbursement from their financial institution occurs in 73% of cases involving bank or credit card fraud. That suggests that settlements agreed between the parties involved are already providing restitution to most victims, whilst the need to set aside money to fulfil their side of the bargain provides an incentive to financial institutions to take steps to avoid fraudulent manipulation of their customers.

CONCLUSION

The failure-to-prevent bribery offense has proved useful to prosecutors, and may have produced at least some incentive for firms to improve corruption prevention procedures. Building on that success, a simple and effective reform would, then, involve enacting clause 4, to create a broader offense of failing to prevent economic crime. By contrast, the proposed extension or replacement of the identification doctrine in clause 5 is controversial, and ironically, puts in question the point of continuing to have failure-to-prevent crimes.

Clause 5 is best dropped until a better relationship between general principles of corporate criminal liability failure-to-prevent offences has been worked out.

AUTHORS

Jeremy Horder

Fellow Jeremy Horder is a professor of criminal law at the London School of Economics in London and a former Law Commissioner for England and Wales.

Gabriele Watts

Fellow Gabriele Watts is a pupil barrister at QEB Hollis Whiteman Chambers in London. She lectures on financial crime to postgraduates at the London School of Economics.

Crypto

Reining in Cryptocurrencies: Has the Horse Already Bolted?

KEITH OLIVER

CAROLINE TIMONEY

Introduction

The UK Treasury is still keen to regulate the cryptocurrency sector and has announced that it will be regulated under the existing financial services regime.

Ministers launched a consultation which ran until April 23 and there are plans to strengthen the FCA to oversee this area, rules on winding down a crypto company and restrictions on selling in the UK market from overseas.

But is this a case of closing the stable door when the horse has already bolted?

The London Tube has been showing adverts for cryptocurrencies for years, celebrities tout the latest coin on Instagram, and adverts at the Super Bowl have advocated for making a quick buck on crypto.

While financial instability abounds, a relic of the last financial crash as well as the results of the COVID-19 pandemic and the Russian invasion of Ukraine, many have been drawn to alternative investment opportunities away from bank regulation and the mainstream organized financial system. If Wall Street, Lehman Brothers, Credit Suisse, Goldman Sachs and so many other big names are now associated with sudden collapses, government bailouts and ever-increasing fees with little gain; cryptocurrencies were seen as an alternative, free of the constraints of the global financial market, without the fine print, controls and secrecy that came to be associated with many financial institutions, and their backroom deals.

However, fine print and controls mean security - whether this is protection for an investment, legal recourse, or accountability. What is evident from the recent crypto collapses, FTX, terraUSD, Luna, Celsius Network, to name a few, is that there is little recourse for investors who buy into the market. Without a globally regulated industry, fraud abounds, and insufficient auditing is taking place. This is a fraudster's paradise!

CREATION OF INTERNATIONAL NORMS

The Financial Action Task Force (FATF) has issued a series of global binding standards in order to regulate the sector and prevent its misuse in terrorist

financing and money laundering. However, few jurisdictions have applied these to their domestic regulatory regimes. As the FATF rightly identifies, this has created serious gaps in the attempt to clamp down on the free-wheeling cryptocurrencies and these have created loopholes exploited by criminals and opportunists.

The FATF standards impose obligations on both countries and virtual asset service providers. Countries are required to recognize the risks of both money laundering and terrorist financing in this sector, are required to supervise the sector, and should licence or register virtual asset service providers. The providers, in turn, are required to set up the same preventative measures as other financial institutions such as customer due diligence, record keeping and reporting of suspicious transactions. They should also obtain and hold beneficiary and originator information alongside virtual asset transactions.

The FATF's Recommendation 16 or "travel rule" was recommended in 2019 to combat the use of cryptocurrencies in money laundering and terrorist financing. The name refers to how the personal data of a transacting party 'travels' with their transfers. The FATF recommends a de minimis threshold of $1,000 (or EUR 1,000) for virtual asset transfers. When transfers exceed this amount, virtual asset service providers (VASPs) must collect:

1. The name of the originator;
2. The originator account number where such an account is used to process the transaction;
3. The originator's address, or national identity number, or customer identification number, or date and place of birth;
4. The name of the beneficiary; and
5. The beneficiary account number where such an account is used to process the transaction.

Countries have been slow to adopt the Travel Rule; however, the recent G7 meeting in Niigata, Japan, supported accelerating the global implementation of FATF standards on virtual assets, per its communique. In the UK, this is implemented in Regulation 5 (on cryptoassets transfers) of the Money Laundering and Terrorist Financing Regulations which will come into force on September 1, 2023.

PROPOSED UK REGULATORY REGIME

The UK is currently in the preliminary stages of regulation. The Treasury announced in February 2023 that it proposes that cryptoassets be regulated within the existing financial services regime. This would ensure that the sector could benefit from the "confidence, credibility and regulatory clarity" set out in the Financial Services and Markets Act 2000 (FSMA). After unveiling its proposals, the Treasury announced a consultation period with stakeholders which finished in April 2023. The Treasury has yet to publish these findings.

In the UK, all cryptocurrency firms such as exchanges, advisors and professionals that either have a presence or market product, or provide services, within the UK market, must register with the Financial Conduct Authority (FCA) under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. Firms that provide cryptoasset services that could constitute 'special investments' are regulated under the FSMA and the FSMA (Regulated Activities) Order 2001.

The FCA reported to the Treasury Committee that 85% of the firms that apply to obtain registration fail as they don't meet the minimum standards required under its anti-money laundering and counter-terrorist financing regime. This has led to accusations from the industry that the UK is stifling innovation; however ActionFraud reports that in 2022 reported losses to crypto-scams rose 72% to more than £329 million. Meanwhile the crypto sector itself showed a collapse in value by approximately 75% from its peak in November 2021. Clearly more stringent regulation is needed.

There have however been questions on whether the industry could be successfully regulated at all. Parliament's Treasury Committee has recently suggested that cryptocurrency trading should be regulated as gambling, rather than as a financial service. The Treasury has also already admitted that some crypto businesses could continue to operate in offshore jurisdictions, bypassing UK regulations.

The government has however included cryptoassets within the Financial Services and Markets Bill (FSMB), which is currently going through the House of Lords and has not yet reached Royal Assent. Proposals include:

1. Including cryptoassets within the financial promotion restriction of s21 of the FSMA;
2. Include cryptoassets within the scope of the regulated activities regime listed in s22 of the FSMA;
3. Introduce a new definition of a cryptoasset as: "any cryptographically secured digital representation of value or contractual rights that (a) can be transferred, stored or traded electronically, and (b) that uses technology supporting the recording or storage of dad (which may include distributed ledger technology).

A more recent amendment offers greater powers to the FCA, expanding its power beyond merely ensuring effective anti-money laundering and financial crime procedures, to treating and regulating cryptoassets similarly to shares and other traditional securities. Cryptoasset firms would need to comply with the full gamut of FSMA regulations, which would include restrictions on how firms advertise and sell in the UK market.

The bill will also empower the Treasury to make regulations which govern payments that include digital settlement assets and their providers. Significant providers will also be brought within the Bank of England's remit, and legislation will be amended so that e-money and payment services will be effective in this regime, including the possibility of fiat-backed stablecoins used for retail. The Bank of England has warned that digital currencies could trigger a financial meltdown unless governments are prepared to formulate tough regulations. However, despite this warning, the Treasury and the Bank have been consulting on whether to set up a UK Central Bank Digital Currency in 2030.

The Treasury published a number of papers in February which highlighted that the government aimed to both protect consumers and encourage innovation with 'proportionate' regulations. The papers clarified that the Treasury believes that cryptoassets should follow the standards of other similar financial services, and that the future regulatory regime will be within the financial services sector. The definition of cryptoassets is aligned with that used by the FATF and the EU.

CASE LAW IN ENGLAND AND WALES

The English courts have taken a prominent role in the attempt to curtail international cryptocurrency frauds. One of the factors that has fueled the rise of this type of criminality is the lack of a defined classification. The unprecedented publication of *The LawTech Delivery Panel Legal Statement on Cryptoassets and Smart Contracts*, distributed by the UK Jurisdiction Taskforce in 2019, suggested that the way to surmount this is to universally class these products as property, as per the statement, *'proprietary rights are recognized against the whole world'*.

This was a world first which formally suggested the blanket covering of cryptoassets as property. A type of English law "land grab" perhaps, it demonstrated the innovative nature of the English courts in their attempt to create an organic and usable tool that applies existing mechanisms to nuanced settings. This approach was endorsed with great success in *AA v Persons Unknown* [2019] EWHC 3556 (Comm), where the High Court granted a proprietary injunction to assist an insurance company in recovering Bitcoin that it had transferred in order to satisfy a malware ransom demand.

There are massive informational gaps when it comes to cryptocurrency, in part due to the anonymity provisions inherent to crypto's design, compounded by the fact that the system is decentralized, and there is no third-party intermediary like a bank or another more traditional financial institution used to validate transactions.

The case of *Ion Science Ltd and Duncan Johns v Persons Unknown, Binance Holdings Limited and Payward Limited* [2020] was the first to consider the lex situs of the cryptocurrency where both the domicile of the beneficial owners and the cryptocurrency exchange were taken into account. This is also mentioned in the case of *Fetch.ai Ltd v Persons Unknown* [2021] EWHC 2254 which solidified the status of the English courts as a leading jurisdiction for resolving crypto disputes and assisting victims of this manner of fraud. In the latter case, the applicants were able to get a Bankers Trust order against the cryptocurrency exchange located outside of England and Wales, as the *lex situ* of a cryptoasset has been determined by the courts to be the place where the person or company who owns the asset is domiciled.

A recent case in this area is *Tulip Trading Ltd v van der Laan* where the Court of Appeal overturned a decision in the High Court and found that there was the possibility of a fiduciary duty of the developers of bitcoin networks to the Bitcoin owners. One of the points made by the court was that "the internet is not a place where the law does not apply." Blockchain technology has often appealed due to its decentralization; crypto as such is not constrained by national institutions. However, if the internet is not above the law, then it is likely that regulation will constrain digital assets and impose obligations on developers in the future.

There have also been attempts to apply other types of law to cryptocurrencies. For example, BSV Claims Limited proposed proceedings under the Competition Act 1998 against Bittylicious Limited and Others. BSV Claims Limited was incorporated as a special purpose vehicle to represent holders of the cryptocurrency Bitcoin Satoshi Vision in a proposed class action in the Competitional Appeal Tribunal. This is the first case of its kind and pits its director, Lord Currie of Marylebone (the first Chair of both Ofcom and the Competition and Markets Authority), representing an estimated 240,000 investors against the exchanges Binance, Bittylicious, Kraken and Shapeshift claiming losses of up to £ 9.9 billion. Bitcoin Satoshi Vision was created in 2018, and a key backer is Craig Wright who has publicly claimed to be the developer of Bitcoin, Satoshi Nakamoto. Wright sued for libel in 2022, winning only nominal damages of £1 after the London High Court ruled he had given false evidence.

By attempting to enhance certainty amidst the confusion, the English courts are sending a clear message that they are a global leader in this domain. Of course, legislation is also trying to keep pace and greater regulatory clarity will be beneficial for consumers, businesses, and the courts alike.

REGULATION IN EUROPE AND THE U.S.

The EU finalised its new Market in Crypto-assets Regulation (MiCA) in 2022. The regulations apply to e-money tokens, asset-referenced tokens, utility tokens and cryptoassets. These categories are quite broad and include cryptocurrency and crypto products which do not fall under existing financial services legislation. Crypto currency without an identifiable

issuer is excluded from MiCA, as are cryptoassets services which are fully decentralized. MiCA has been applauded as a broad, coordinated regulatory framework for cryptoassets across Europe, and has been singled out as a regime that the U.S. should seek to emulate.

At a May 10, 2023, hearing on the future of digital asset regulation, U.S. lawmakers highlighted the MiCA framework, as well as the proposed UK regulations, as a comprehensive package in opposition to the current U.S. hodgepodge (Wright, 2023). U.S. regulators, such as the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission, have been competing for prominence in this space. The industry is currently governed through existing federal securities, derivatives and banking laws and the recent crackdown by U.S. regulators against large cryptocurrency exchanges has led to a request for greater clarity.

CONCLUSION

The UK, having observed the EU's approach to crypto, has proposed that the industry fall within the ground rules set up for the existing financial services framework. Although there has been some support for the government's proposals, there has also been some disquiet for this legitimization of the industry.

For example, the Institute of Chartered Accountants in England and Wales supported the initiatives but warned that the risk to consumers remained in their consultation. Other groups asked for more precise definitions of what the regulations would cover, and how these transactions would be taxed. Clearly there are identifiable gaps which the consultation period has raised. The government's promise to completely regulate the industry by the end of 2023 appears somewhat rash but a regulatory regime for cryptoassets would definitely be timely and welcomed by those suffering in its uncertainties. Binance's approval of the UK proposals is helpful in encouraging other crypto institutions to comply with the forthcoming regulations.

Despite the ambition of the Treasury the horse may have already bolted. The proposed UK regulatory regime is also vulnerable without international support, and that horse may just find another stable in another jurisdiction with greener grass.

AUTHORS

Keith Oliver

Fellow Keith Oliver is head of the international practice at Peters & Peters in London. He specializes in commercial, regulatory and trust litigation.

Caroline Timoney

Caroline Timoney is a commercial litigation and civil fraud legal researcher at Peters & Peters in London.

Fin Crime

ESG and Financial Crime - a European Perspective

DAVID S. SCHREUDERS

Introduction

The Environmental, Social and Governance (ESG) domain has become quite dominant in the international business and legal landscape in the past few years. In short, ESG relates to non-financial performance indicators for an investment or a business and makes it possible to assess the impact on the earth, in terms of sustainability and ethics, from the way companies act. Sustainability in business refers to a company's strategy to reduce negative environmental impact resulting from their operations in a particular market and ESG metrics are helpful in that respect to analyze the company's practices.

An equivalent to the term ESG is "corporate social responsibility," which has found its reflection in a number of principles on business and human rights, laid down in guidelines from the UN and the OECD. These guidelines are to be considered as "soft law"': they are basically a set of non-binding best practices. Since a few years we are seeing a shift to "hard law", for example, in a huge legislative operation in the EU, imposing mandatory rules and requirements on businesses inspired by the business and human rights soft law guidelines. And when it comes to legal obligations, there is always an enforcement side to it.

This article discusses the possible role of financial crime enforcement in order to achieve ESG goals.

THE EUROPEAN UNION AS DRIVING FORCE BEHIND ESG LEGISLATION

On January 5, 2023, the EU Corporate Sustainability Reporting Directive (CSRD) came into force, which will now have to be implemented in the laws of the member states. With this directive the European Commission aims to expand its sustainability disclosure requirements for large companies. The CSRD requires reporting on (inter alia) several aspects of dealing with sustainability matters, such as the resilience of the business model and strategy, how impacts on sustainability matters are taking into account, the due diligence process and actions taken to prevent, mitigate or end adverse impacts. "Sustainability matters" is being defined as environmental, social

and human rights, and governance factors, including sustainability factors in the meaning of the EU Sustainable Finance Disclosure Regulation (SFDR), namely environmental, social and employee matters, respect for human rights, anti-corruption and anti-bribery matters. The SFDR of November 27, 2019, seeks to achieve more transparency regarding how financial market participants and financial advisers integrate sustainability risks into their investment decisions and investment or insurance advice.

Very recently, on June 1, 2023, the European Parliament approved with 381 amendments to the text, the February 2022 proposal from the European Commission for a Corporate Sustainable Due Diligence Directive (CSDDD). This directive aims to ensure that companies active in the internal market contribute to sustainable development and the sustainability transition of economies and societies by respecting human rights and the environment. It is considered essential to establish a European framework for a responsible and sustainable approach to global value chains, because companies are an important pillar in the construction of a sustainable society and economy. The due diligence process set out in this directive should cover the six steps defined by the OECD Due Diligence Guidance for Responsible Business Conduct. Beside a strong focus on the respect for human rights, the directive is in the eyes of the European Parliament also an important legislative tool to avoid any misleading climate neutrality claims and to stop greenwashing and fossil fuels expansion worldwide in order to achieve international and European climate objectives.

In respect of combating and reducing the risk of greenwashing, the European Commission published on March 22, 2023, a proposal of the so-called Green Claims Directive (GCD), which will be discussed later.

All these EU legislation initiatives should be seen in the context of the European Green Deal (2020), a legislative roadmap and the "Fit for 55" package, both aimed at reaching carbon emissions reduction in 2030 with 55% as compared to 1990 and making the EU climate-neutral in 2050. Unlike the upcoming trend of ESG "backlash" which can be perceived in the US – examples are the Florida Act Relating to Government and Corporate Activism as of May 1, 2023, which prohibits investment plans based on non-pecuniary factors, including ESG factors; furthermore, using antitrust law as a potential counter to ESG efforts by companies who are coordinating actions to combat

climate change – the ESG legislation in Europe is developing fast and it has a relevance to all industry sectors.

I will now discuss the possibilities of reaching ESG goals by making use of enforcement through financial crime provisions.

COMMON CRIMES IN AN ESG CONTEXT

The broad European sustainability approach within ESG makes it relatively simple to point out crimes which could be qualified as 'classic crimes' being relevant in the scope of ESG enforcement. Within the environmental domain, all kinds of environmental crimes would fall within this spectrum: fraud with hazardous waste, fraud with chemical substances, illegal or improper use of pesticides, oil spills, illegal fireworks trade, illegal trade in protected species, fraud with use of manure in farming, all kinds of duty of care violations relating to occupational hazards. The Netherlands has a strong tradition of environmental crime prosecutions since the 1980's and specialized prosecutors and investigation teams are effective in law enforcement in this area. Prosecuting groups of individuals and companies charging them with the serious crime of being a criminal organisation in an environmental crime context is quite common in the Netherlands.

As regards Social, examples of common crimes are child labor, forced labor and modern slavery.

Examples of crimes in the governance space are tax fraud, bankruptcy fraud, violation of economic and trade sanctions, anti-money laundering due diligence violations and corruption. With respect to the latter, as noted in the above, apart from environmental, social and employee matters, and respect for human rights, anti-corruption and anti-bribery matters have explicitly been identified as sustainability factors in the EU SFDR en CSRD. One of the previously mentioned amendments by the European Parliament in the proposed CSDDD is amendment 32, which adds a new recital (25d) to the directive, reading: *"Adverse human rights and environmental impacts can be intertwined or underpinned by factors such as corruption and bribery, hence their inclusion in the OECD Guidelines for Multinational Enterprises. It therefore may be necessary for companies to take into account these factors when carrying out human rights and environmental due diligence."*

In a European context, effective and robust compliance programs are, also from an ESG perspective, becoming more and more important in order to avoid criminal liability for both corporations and their management.

SPECIFIC ESG CRIMES

An example of a specific ESG crime could be found in Article 4 of the EU regulation laying down the obligations of operators who place timber and timber products on the market (Timber Regulation, 2010). The placing on the market of illegally harvested timber or timber products derived from such timber is prohibited and operators shall exercise due diligence when placing timber or timber products on the market. To that end, they will have to use a due diligence system as set out in Article 6 of the Regulation. In December 2022, a Dutch company was convicted by the Criminal Court of Amsterdam for violating this regulation because of involvement in importing teak wood from Myanmar in the Czech Republic without executing the required due diligence.

A second example is the EU regulation on ship recycling (2013), which has the purpose to protect human health and the (marine) environment. Currently, German public prosecutors are investigating persons suspected of illegally dismantling ships. Apparently, they are looking into alternative routes for prosecution, now that the German legislator had failed to enact a criminal law sanctioning the violation of the regulation. In the Netherlands, companies have been convicted in 2018 for violation of the EU regulation on shipments of waste (2016). In the eyes of the Dutch Court, the entire ship which made its final journey to a beach in Bangladesh in order to be dismantled there, could be considered “waste” under the 2016 Regulation, which provisions had not been followed.

Soon, the EU Deforestation Regulation (EUDR) which will come into force on June 29, 2023, will expand the spectrum of specific ESG violations. From December 30, 2024, it is prohibited to place or make available on the EU market (but also to export from that market) commodities and products listed in Annex I to this regulation (palm oil, soya, wood, cocoa, coffee, cattle and rubber), unless they are deforestation free, they have been produced in accordance with “ESG-laws” in the country of production and they are covered by a due diligence statement which is the justified outcome of

an extensive due diligence process. The EUDR contains a comprehensive enforcement system with elements which could lead to putting criminal enforcement in place by the member states.

ECOCIDE

Not only financial crime-related because it can also be positioned in the scope of international law, is "ecocide", the mass damage and destruction of the natural living world. It has not been codified as a separate crime in international law yet but an independent Expert Panel for the Legal Definition of Ecocide drafted as legal definition in June 2021: *"Unlawful or wanton acts committed with knowledge that there is a substantial likelihood of severe and either widespread or long-term damage to the environment being caused by those acts"*. Discussions are currently going on about possible ecocide in the war in Ukraine, but also actions by corporates could, in the view of some countries, qualify as ecocide. Those countries include France, Belgium, Finland and the UK, where on a national level codification of ecocide is being discussed.

GREENWASHING

The proposed Green Claims Directive (GCD) as of March 22, 2023, aims at protecting consumers from greenwashing, when corporations make misleading claims about their green credentials and when those credentials are marketed as being more sustainable than they really are. It is important to note that the GCD only deals with voluntary environmental claims and is limited to environmental labels only. Social aspects are not being covered by this directive. "Green claims" must be substantiated and this substantiation should be verified afterwards.

Article 17 of the proposed directive deals with penalties, which should be "effective, proportionate and dissuasive." The GCD furthermore explicitly prescribes that member states shall provide that penalties and measures for infringements of this directive shall include (a) fines which effectively deprive those responsible of the economic benefits from their infringements, (b) confiscation of revenues and (c) temporary exclusion from public

procurement processes and from access to public funding. Member states are supposed to have a certain form of freedom when implementing the directive, but as regards penalties it is the element of "confiscation" which makes this question interesting from an enforcement point of view.

Not all EU countries have legal confiscation powers in their administrative (regulatory) domain – the Netherlands for example, is such a country. Confiscation as such is only possible in the context of criminal enforcement; regulators (depending on the specific regulatory legislation) can impose maximum fines which reflect 10% of the annual turn-over of a corporate, but this could be qualified as a "fine which effectively deprives those responsible of the economic benefits", in the meaning of element (a) of Article 17.

It is therefore interesting to see how the penalties for infringements of the GCD, especially when an element of misleading (fraud) is involved, will be implemented throughout the EU. Because the GCD only covers greenwashing in terms of false environmental claims, when traders would make social claims ('no child labor' for example) and this could be considered as intentionally misleading the consumers, in my view this would qualify as fraud or misrepresentation and could be prosecuted as a serious crime in a criminal court.

The way infringements of the GCD will be implemented in national laws of the EU member states with "dissuasive" penalties, is also relevant for the next issue to be discussed: if the violation could be a legal ground for money laundering prosecution.

MONEY LAUNDERING AND LAUNDERING OTHER OBJECTS

Many EU countries, including the Netherlands, have a money laundering provision which could be considered a catch-all provision: every imaginable action which could be applied to an object originating from serious crime, is punishable (disguising, concealing, obtaining, possessing, using, transferring, etc.). In order to create harmonisation in the EU, the directive on combating money laundering by criminal law (2018) has indicated 22 crimes as criminal activity which form the basis for a money laundering offense

when committed with intent. Human trafficking, sexual exploitation and environmental crime are ESG-related crimes on that list.

Another important factor to take into account in terms of risk management is the extended jurisdiction issue. According to Article 3, par. 3(c) of the directive, the money laundering offense extends to property derived from conduct that occurred on the territory of another member state or of a third country, where that conduct would constitute a criminal activity had it occurred domestically. In an ESG context this would mean that when a product would be manufactured with child labor, which is punishable in the EU member state, but not in the third country, the money derived from the child labor activity would be captured by the money laundering offence when committed with intent. This will open the way for intentional money laundering prosecutions in an ESG context, relating to ESG related crimes which are punishable within the EU but are not in a third country.

Finally, legal practice shows that it is not always money which is being laundered in an ESG context. In 2019, a Dutch fishing company was found guilty for knowingly and willingly laundering shells, illegally caught in the North Sea by another fishing company. Dutch newspaper NRC reported on June 2 about a joint investigative journalism inquiry on Brazilian prime beef, conducted together with journalists' collective Forbidden Stories. This product came from cattle raised on pieces of land that were created by illegal deforestation in the Brazilian Amazon territories. It appeared that due to the Brazilian system, it was possible to move cattle around to several farms (sometimes 3 to 6) and that only the final farm – which is situated on legal soil – will be assessed by slaughterhouses. This is basically a clear example of "layering" as we know it in the context of money laundering, in order to disguise the illicit origin of the meat.

CONCLUSIONS

The EU legislation on ESG topics is comprehensive, covers all sectors and forces (in principle: large) corporations to enhance their due diligence processes and to keep up with increasing compliance requirements. The mandatory laws and regulations could to some extent also be enforced through already existing financial crime provisions. In this respect, criminal enforcement

is not new, but the ESG focus could lead to renewed enforcement actions from European regulators. Corporations should therefore not only take civil or regulatory enforcement actions into account, but should also be aware of criminal enforcement risks.

Especially because of the broadened scope of the intentional money laundering offense in the EU, in an ESG context prosecution within the EU could arise, relating to predicate ESG related offenses which are not punishable in the third country where the ESG infringement takes place. Also in this respect, corporations should be aware of financial crime risks and continue to work on improving their compliance programs in order to mitigate liability risks.

AUTHORS

David S. Schreuders

Fellow David S. Schreuders is a partner with Simmons & Simmons in Amsterdam. He focuses on financial and economic criminal law.

Clawbacks

Compensation Clawbacks: Domestic and International Considerations of DOJ Pilot Program

DIANA K. LLOYD

MEG E. ZIEGLER

Introduction

Compensation recoupment programs, or "clawbacks," can be an effective means for promoting individual accountability, but have historically been utilized inconsistently throughout the global economy. Recent announcements from the Department of Justice indicate a renewed focus on compensation-based efforts to deter fraud and wrongdoing in the United States, but enforcement of such efforts here and abroad remains an open question.

DOJ'S CLAWBACKS PILOT PROGRAM

On March 2, 2023, Deputy Attorney General Lisa Monaco announced a three-year Pilot Program Regarding Compensation Incentives and Clawbacks. By focusing on compensation, the Pilot Program is aimed at broadening the burden of responsibility for corporate wrongdoing and the resulting financial penalties to include the individuals deemed responsible as well as a company and its shareholders to. The Pilot Program effectuates policies outlined in a September 2022 DOJ memo, "Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Groups" and exemplifies DOJ's continued focus on individual accountability.

The Pilot Program has two parts and is focused both on incentivizing good compliance practices and financially penalizing individuals involved in misconduct. First, companies entering into criminal resolutions with DOJ "will be required to implement compliance-related criteria in their compensation and bonus system." DOJ prosecutors are instructed to use discretion in tailoring appropriate requirements to the facts and circumstances of the particular case, including applicable foreign and domestic laws.

Second, companies will be eligible for fine reductions commensurate with any compensation they are able to recoup from culpable individuals. The clawback arm of the Pilot Program specifically provides that "an additional fine reduction may be warranted" if (1) "a company fully cooperates and timely and appropriately remediates and demonstrates it has implemented a program to recoup compensation from employees who engaged in

wrongdoing in connection with the conduct under investigation, or others who both (a) had supervisory authority of the employee(s) or business area engaged in the misconduct and (b) knew of, or were willfully blind to, the misconduct," and (2) *"has in good faith initiated the process to recoup such compensation before the time of resolution . . ."* (emphasis added). The fine reduction shall be equal to the amount the company is able to successfully claw back. In addition to the discounted fine, the company gets to retain the recouped compensation.

Where companies' good faith attempts to claw back compensation are unsuccessful, the Program gives prosecutors discretion to offer a fine reduction of up to 25% of the amount the company attempted to recoup. DOJ's guidance provides that the reduction "may be warranted where, for instance, a company incurred significant litigation costs for shareholders or can demonstrate that it is highly likely that it will successfully recoup the compensation after the end of the resolution term."

As for how this will look in practice, at the time of entering into the criminal resolution, companies will pay the full amount of the applicable fine, less 100% of the amount they are going to attempt to claw back (the "Possible Clawback Reduction"). At the end of the resolution term, the company will need to pay the Possible Clawback Reduction, less either (1) 100% of any compensation the company was successfully able to recover, or (2) the determined percentage of the reduction allotted due to good faith, but unsuccessful, efforts.

The Program went into effect on March 15, and will be evaluated in three years to determine if it should be extended or modified.

ADDITIONAL POLICY UPDATES

DOJ's Principles of Federal Prosecution of Business Organizations have also been updated to reflect a renewed focus on clawbacks as a key component of an effective compliance program that holds culpable individuals accountable. Section 9-28.800 (Corporate Compliance Programs) directs prosecutors to "consider whether the corporation's compensation agreements, arrangements, and packages (the 'compensation systems')

incorporate elements—such as compensation clawback provisions—that enable financial recoveries and penalties to be levied against current or former employees, executives, or directors whose direct or supervisory actions or omissions contributed to criminal conduct." Furthermore, DOJ is focused not only on the existence of such provisions, but also on whether companies actually utilize them: "if a corporation has included clawback provisions in its compensation agreements, prosecutors should consider whether, following the corporation's discovery of misconduct, a corporation has, to the extent possible, taken affirmative steps to execute on such agreements and clawback compensation previously paid to current or former executives whose actions or omissions resulted in, or contributed to, the criminal conduct at issue."

CORPORATE INTEGRITY AGREEMENTS

This focus on compensation clawbacks as a compliance mechanism harkens back to 2012, when provisions similar to those contemplated by the Pilot Program began appearing in Corporate Integrity Agreements (CIAs) with the federal government. For example, in July 2012, GlaxoSmithKline (GSK) entered into what was at the time the largest health care fraud settlement in U.S. history and a five-year CIA that required GSK to "establish and maintain . . . a financial recoupment program that puts at risk of forfeiture and recoupment an amount equivalent to up to 3 years of annual performance pay (i.e., annual bonus, plus long term incentives) for an executive who is discovered to have been involved in any significant misconduct." This "Executive Financial Recoupment Program" was to apply to current and former GSK employees at the time of a "Recoupment Determination." Similarly, Johnson & Johnson entered into a CIA in 2013 that required the creation of a comprehensive Executive Financial Recoupment Program, covering both incentive compensation and unvested equity awards, within 150 days of the Effective Date of the CIA. Similar programs have appeared in a number of CIAs in subsequent years.

PRACTICAL CONSIDERATIONS

The Pilot Program incentivizes companies to proactively modify or create—and, importantly, utilize—clawback policies, such that they are eligible for fine reductions at the time of entering into criminal resolutions, rather than retroactively as part of a CIA after a settlement. Those companies looking to overhaul their compensation systems in light of the Pilot Program can gain insight into how best to do so by looking to the Executive Financial Recoupment Programs as outlined in prior years' CIAs as well as the new guidance around the Pilot Program.

Clawback policies incorporated into employment agreements, offer letters, severance agreements, and bonus, equity, and incentive plans need to contemplate not only the DOJ's new guidance, but also the requirements of the Securities and Exchange Commission's (SEC) Dodd-Frank Wall Street Reform and Consumer Protection Act, new rules for which were officially adopted on January 27, 2023. The SEC's rules require companies to "develop and implement a policy providing for the recovery, in the event of a required accounting restatement, of incentive-based compensation received by current or former executive officers where that compensation is based on erroneously reported financial information. The listing standards must also require disclosure of the policy." The SEC first proposed such rules in 2015, so many companies may already have clawback policies tailored to this unique and slightly narrower set of circumstances than what is contemplated by the Pilot Program.

The Pilot Program also leaves open a number of questions around its reach and enforcement. First, what individuals fall within its scope? While it is clear those individuals who were directly responsible are subject to the Program's terms, it remains an open question to what extent compliance personnel, supervisors, or upper-level management will be considered to have knowledge of the conduct at issue or to have been "willfully blind" such that they too are vulnerable to clawbacks.

Second, domestic and international wage and hour laws may make it difficult for companies to implement and act upon clawback policies. In the United States, different states provide varying levels of protection for employee wages. Typically, once a wage is "earned," it cannot be clawed

back, but whether compensation such as equity awards, bonuses, or commissions is considered a wage varies by state. Foreign laws may afford even greater protection to employees. Non-US companies that are subject to the jurisdiction of the Department of Justice due to, for example, trading shares on a United States stock exchange will need to figure out how to reconcile the laws of their home country with the DOJ's expectations under the Pilot Program. Similarly, US-based companies may have employees from all across the globe who fall within the purview of the Pilot Program, but attempting to claw back compensation from those individuals will require navigating a complex international legal and regulatory scheme. Still other companies may already find themselves on solid ground with respect to the Program because their home countries already require recoupment programs for their industry.

Third, and relatedly, it is not clear when a company's "good faith" attempts to recoup compensation would qualify it for a partial fine reduction. It is one thing to implement a compensation program that aligns with DOJ's expectations, but quite another to enforce that program in practice. DOJ acknowledges that attempts to claw back compensation may lead to costly litigation and/or take longer than the allotted three-year window, but provides little other guidance about what would constitute good faith. This is a particularly important consideration for companies that, as described above, have to weigh the costs of navigating a complex international legal scheme in order to recoup employee compensation.

CONCLUSION

Companies should take this opportunity to evaluate their existing compensation systems and implement compliance-based metrics and clawback policies. Companies that find themselves subject to a government investigation will likely face a renewed focus on individual employees and executives, leading to a difficult balancing of individual rights and company interests. The Pilot Program raises difficult questions about whether the costs of changing compensation policies and pursuing clawbacks—costs that include not only dollars and cents, but also the impact such actions will have on employees—are worth the benefit of a potential fine reduction. Furthermore, who falls within the scope of the Pilot Program, what constitutes

good faith efforts to recoup compensation, and the enforceability of the Program under a particular state or country's labor and wage laws are open questions that we will likely see play out as implementation of the Program gets underway. The myriad challenges to effecting clawbacks both within the U.S. and globally may well mean that we see very few clawbacks under the Pilot Program.

AUTHORS

Diana K. Lloyd

Fellow Diana Lloyd is co-chair of Choate's government enforcement and compliance group in Boston. She specializes in government enforcement matters and internal investigations.

Meg E. Ziegler

Meg Ziegler is an associate in Choate's government enforcement and compliance group in Boston. Her practice focuses on complex litigation and government and internal investigations.

Forfeiture

A Swiss–Peruvian Asset Recovery Case Boosts Prospects for Non-Conviction Based Forfeiture in the Fight Against Transnational Corruption and Money Laundering

OSCAR SOLÓRZANO
GRETTA FENNER

Introduction

Switzerland is set to return $8.5 million to Peru in a precedent-setting case of non-conviction based forfeiture. A decision by the Swiss Federal Supreme Court on April 25, 2023 cleared the way for the return of the corruptly obtained assets to Peru. The money to be returned is part of a group of cases linked to Vladimiro Montesinos, Head of Intelligence under former President Alberto Fujimori. The funds have been frozen in a Zurich bank account for nearly 20 years.

It is a highly symbolic case for both Switzerland and Peru and sets an important precedent for the use of non-conviction based forfeiture laws to recover illicit assets arising from corruption. Such laws allow for the recovery of illicit assets outside of criminal proceedings, usually but not always through an independent judicial process that applies civil rules and is directed against the asset itself (in rem). Many variations exist. U.S. civil judicial forfeiture is an example of non-conviction based forfeiture that was originally developed to recover property from pirates and slave traffickers, and is now used to confiscate assets linked to various forms of crime.

Non-conviction based forfeiture laws have existed for many years in several countries in a wide variety of forms, and are encouraged in various international treaties. However, their diversity – and the fact that many countries still do not have or use such laws – leads to challenges with their application, especially in cases with an international element.

The Swiss-Peru case has three main takeaways for those involved in international financial crime litigation and asset recovery proceedings:

- First, non-conviction based forfeiture is an innovative and promising tool in the fight against corruption. It makes it possible to get at the "untouchables", or at least the money they have stolen, even when the criminal justice system fails to convict a person for whatever reason. Peru's successful application of this legal tool has already inspired other asset recovery practitioners far beyond Peru or even Latin America.

- Second, the case shows the merits of states (in this case Switzerland) being open to novel asset recovery mechanisms so as to be able to offer help in the context of international judicial cooperation. Other large

financial centers can take note. As we at the Basel Institute regularly promote in policy forums and among our partner governments, all states should live up to their international commitments to provide the widest possible measure of international cooperation in asset recovery.

- Third, victim states seeking to recover assets internationally through NCBF laws must implement laws and practices that are compatible with international standards, including human rights standards. This point is closely linked to the ability of the requested state to cooperate in the prosecution and in the enforcement of NCBF decisions. Victim states also need the technical competence to conduct complex cases, which may be gained through experience over time.

MULTIPLE APPEALS FROM A MAN WHO FLED PROSECUTION

The Peruvian case discussed in this paper is an example of the last point. Despite the relatively small amount of money – at least compared to the amount stolen through corruption over the years – it was a challenging case.

Based on a detailed financial investigation, our Peruvian prosecutor partners were able to prove in court that the $8.5 million was derived from corrupt contracts for the purchase of overvalued fighter jets from Belarus during Peru's Fujimori government. The beneficial owner of the Zurich bank account was German-Israeli businessman Moshe Rothschild Chassin, an accomplice of Montesinos. He fled to Israel to evade prosecution and, despite being subject to an Interpol red notice, remains free.

In 2021, after Peru's courts issued the forfeiture order, the judicial authorities sent a mutual legal assistance (MLA) request to the Swiss authorities to execute the confiscation order and return the money.

Rothschild Chassin challenged the forfeiture order at all appeals stages in Switzerland: in the Attorney General's Office in Zurich, in the Federal Criminal Court in Bellinzona and in the Federal Supreme Court in Lausanne.

The Swiss judges agreed with their Peruvian counterparts that the information revealed through a detailed financial investigation was sufficient to prove that the bank account in Zurich constituted proceeds of crime. Second, they rejected the appeals, noting that the non-conviction based forfeiture procedure in Peru had been conducted in accordance with all applicable standards and legal rights.

UNTAPPED POTENTIAL OF NON-CONVICTION BASED FORFEITURE LAWS

The Peruvian forfeiture order was based on its Extinción de dominio law, a form of non-conviction based forfeiture law that is quite prevalent across Latin America. The Peruvian Extinción de dominio law, which was introduced in 2018, implements an independent procedure that occurs outside criminal proceedings and applies a civil standard of proof. As an in rem action, it enables the forfeiture of assets linked to corruption or other crimes where criminal proceedings are not possible or desirable.

This was the case for Rothschild Chassin. As an accomplice rather than a public servant, he can never be prosecuted on criminal charges of collusion and bribery. As an Israeli citizen, he will also not be extradited from Israel to face criminal charges in Peru.

Various judicial mechanisms are in place to ensure that the person's rights are fully respected throughout the process, namely the right to property and the right to a fair trial.

Its *Extinción de dominio* law is one reason why Peru has become a positive role model in the region in terms of asset recovery. At a recent convention of judges organized by the Basel Institute's team in Lima, the Head of Peru's Judiciary Javier Arévalo Vela highlighted that the law had already enabled the recovery of around $64 million in illicit assets, with many more cases in the pipeline.

Speaking about the case, Peruvian Judge Eduardo Torres explained that "it is also important for the Peruvian justice system as a whole. The fact that money misappropriated from the Peruvian treasury will be returned shows

we are in compliance with international treaties. And we are sending a message to the corrupt: if you misuse the public administration and steal Peruvian money, ultimately you will not profit from it."

INTERNATIONAL COOPERATION

International cooperation is a constant challenge for countries seeking to recover corrupt assets, as Peruvian Specialized Prosecutor Hamilton Castro explained in this interview. In too many cases, states harboring illicit assets will not cooperate on cases where they do not have an equivalent asset recovery mechanism.

As will be explained in a forthcoming Basel Institute on Governance Working Paper, the lack of harmonization of non-conviction based forfeiture mechanisms has resulted in countries in Latin America (and elsewhere) having limited success in obtaining international cooperation through MLA in such cases. This negatively affects victim states' ability to freeze and confiscate suspect assets held abroad, and as a consequence negatively affects global efforts to combat corruption and illicit financial flows.

This situation is particularly problematic in the international enforcement of confiscations, although it would be fair to point out that several international financial centers, such as Switzerland or Luxembourg, have taken decisive steps in clarifying the requirements to enforce NCBF decisions from overseas.

Though Switzerland does not have a comparable (autonomous and independent) non-conviction based forfeiture law, it has shown willingness to evaluate Peru's law according to its own legal principles and offer assistance where possible. This indicates that Swiss judges have no issue in principle with civil laws targeting illicit assets, as long as they are clearly not punitive in nature and properly respect human rights. As long as the application of an NCBF law does not entail a penalty or sanction on an individual, civil standards can apply. These include the standard of proof (balance of probabilities), non-application of the prohibition on retroactivity and statute of limitations, and non-application of other principles designed for criminal trials such as protection from self-incrimination and double jeopardy. Judges in the European Court of Human Rights have come to similar conclusions

(see for example Box 2 in a recent case study on another non-conviction based forfeiture case involving Peru and Switzerland).

The considerations of the Swiss Criminal Court can be best explained by a look into its decision of April 4, 2023.

It rejects the claim that the forfeiture violates the prohibition against retroactivity. The Extinción de dominio law is a *restorative* type of law that restores the legal situation to how it was before the commission of a crime (status quo ex ante). It is not a penalty nor does it presuppose a guilty verdict. The prohibition of retroactivity has been designed for criminal procedure; thus, it does not in principle apply in non-conviction based forfeiture;

It also rejects the claim that the offenses in question are time-barred under both Swiss and Peruvian law, which would mean that the statute of limitations applies. The decision points out that the statute of limitations is not mentioned in the Swiss-Peruvian MLA treaty and therefore does not need to be examined before MLA can be provided.

WHAT'S NEXT?

The funds will be transferred to Peru and used in a manner to be agreed upon between the two concerned jurisdictions. Over $25 million confiscated by Peru previously in this complex of cases were returned under a trilateral agreement in 2020 between Switzerland, Luxembourg and Peru that foresees the use of funds to strengthen the country's law enforcement and judicial systems.

Beyond the legal precedents set in relation to the Swiss decisions, we also note that Peru's judicial authorities have gained knowledge and confidence in applying this law and having confiscation orders executed internationally. We also see prosecutors and judges in other Latin American countries empowered by the positive example set by Switzerland and Peru.

At the Basel Institute, we promote asset recovery mechanisms globally that are effective, but also proportionate and respectful of human rights. We believe these are the ingredients to make these laws truly global legal tools in the fight against corruption and other forms of crime.

AUTHORS

Oscar Solórzano

Oscar Solórzano is the Basel Institute's head of Latin America and a senior asset recovery specialist. Working closely with authorities in Peru and across Latin America, as well as global financial centers, he has driven step changes in governments' capabilities to recover proceeds of corruption from overseas jurisdictions.

Gretta Fenner

Founding Fellow Gretta Fenner is the managing director of the Basel Institute on Governance and its International Centre for Asset Recovery in Basel. She is a well-known voice internationally on matters of anti-corruption and asset recovery.

The International Academy of Financial Crime Litigators Founders

For further information, please consult our website:
www.financialcrimelitigators.org

STÉPHANE BONIFASSI
Bonifassi Avocats

LINCOLN CAYLOR
Bennett Jones

ELIZABETH ORTEGA
ECO Strategic Communications