2021 Research report

Money Laundering and Whistleblowers

Giancarlo Spagnolo
Theo Nyreröd

SNS

Money Laundering and Whistleblowers

Money Laundering and Whistleblowers

Giancarlo Spagnolo
Theo Nyreröd

SNS
Box 5629, 114 86 Stockholm
Phone: +46 8-507025 00
info@sns.se www.sns.se

SNS, the Center for Business and Policy Studies, is an independent, non-profit organization founded in 1948 that aims to be Sweden's leading platform for objective debate and knowledge-sharing among decision-makers on key societal issues. SNS brings together representatives from the business community, public sector, academia, and politics. SNS takes no positions on policy issues, which supports its bridge-building role. Members include companies, public authorities, and organizations.

Money Laundering and Whistleblowers
Giancarlo Spagnolo and Theo Nyreröd

Print: Books on Demand, Germany
ISBN 978-91-88637-69-7

CONTENTS

ACKNOWLEDGMENTS

We are grateful to the reference group and in particular to Mats Bergman, Ulrika Mörth, Nicklas Lundh, Christian Lynne Wandt, and Cecilia Wolrath Ekenbäck for their extremely valuable comments and suggestions. Of course, all remaining mistakes are our own responsibility. The SNS staff offered excellent organizational and editorial support.

Giancarlo Spagnolo *Theo Nyreröd*

LIST OF ABBREVIATIONS

AML	Anti-Money Laundering
CTF	Counter-Terrorist Financing
DOJ	United States Department of Justice
EBA	European Banking Authority
FATF	Financial Action Taskforce
FCA	False Claims Act
FIU	Financial Intelligence Unit
FSA	Financial Services Authority
IRS	United States Internal Revenue Service
KYC	Know Your Customer
MER	Membership Evaluation Report
NDA	Non-Disclosure Agreement
SEC	United States Securities and Exchange Commission

Foreword

IN THIS REPORT Giancarlo Spagnolo, professor of economics at the Stockholm Institute of Transition Economics (SITE) at the Stockholm School of Economics, and Theo Nyreröd, PhD candidate at Brunel Law School, provide an overview of anti-money laundering deficiencies in banks by describing a number of recent cases in relative detail. They go on to review the development of the regulatory framework regarding money laundering and the institutions implementing and supervising it.

Their analysis leads them to look into another enforcement and supervision method for use in severe and protracted cases of anti-money laundering non-compliance: incentivizing whistleblowing by offering financial rewards funded by fines and recovered assets. In doing this, the authors cover the practice of whistleblower reward programs in the United States — that were recently extended to money laundering—and what the academic literature has shown about their effectiveness.

SNS hopes that this study can contribute to contemporary debates on how to effectively organize anti-money laundering activities.

The authors are solely responsible for the analysis, conclusion, and policy advice presented in the report. SNS as an organization does not take a position on any of the perspectives offered by the review. The mission of SNS is to initiate and present research-based analyses of issues of importance for society.

The project has been made possible through funding from a reference group that also has been following the research project. The reference group consists of Deloitte, Finansinspektionen, Länsförsäkringar, Mannheimer Swartling, SEB, Swedbank, Swedish Bankers' Association, Swedish Police Authority (National Operations Department), and Swedish Prosecution Authority. Per Strömberg, professor of finance

at the Stockholm School of Economics, is the SNS Scientific Council's representative in the reference group. The authors have received valuable input and comments on earlier drafts of the report from the members of the reference group.

At an academic seminar, Mats A. Bergman, professor of economics at Södertörn University, and Ulrika Mörth, professor of political science at the Stockholm University, provided constructive comments on the report.

The summary of the report has been translated into Swedish by Theo Nyreröd in collaboration with SNS.

Stockholm in October 2021

Stefan Sandström
Research Director, SNS

Swedish Summary / Svensk sammanfattning

I SLUTET AV 1980-TALET blev penningtvättsbekämpningen en prioritet på den internationella dagordningen. Det första europeiska penningtvättsdirektivet antogs 1991 och trettio år senare – och med ytterligare fyra direktiv på plats, samt två till på väg – tycks problemet med penningtvätt vara lika aktuellt som någonsin förr. Det uppmärksammade fallet med den brittiska bankkoncernen HSBC, där drogkarteller under flera år påstås ha haft möjlighet att tvätta pengar på grund av bristen på regelefterlevnad, har följts av fler upptäckta brister i många andra europeiska och nordiska banker.

Finansinstitut påpekar ofta att regelverket mot penningtvätt är komplext och att reglerna för riskbedömning inte har beskrivits tillräckligt utförligt, samt att de dessutom anpassar sig till ett landskap i ständig rörelse (vilket sex direktiv är ett bevis på). Samtidigt tycks europeiska beslutsfattare och experter vara överens om att den nuvarande tillsynen inte är tillräckligt effektiv, till exempel när det gäller återvinning av tillgångar, och många har efterlyst bättre tillsyn och tillämpning av reglerna.

Med tanke på de påstådda höga implementeringskostnaderna och den begränsade effektiviteten i det nuvarande regelverket mot penningtvätt i Europa borde nya tillsyns- och lagföringsmetoder vara välkomna. I USA har man nyligen infört en ny metod på detta område. Metoden går ut på att erbjuda ekonomiska belöningar, finansierade med böter och återvunna tillgångar (otillbörliga vinster), till visselblåsare som ger särskilt värdefull information om allvarliga fall av bristande efterlevnad till tillsynsmyndigheter eller brottsbekämpande myndigheter. Det huvudsakliga syftet med denna rapport är att bedöma hur genomförbar den metoden skulle vara i Europa. Nedan följer några av rapportens centrala slutsatser.

Slutsatser från fallstudier

Efter att ha genomfört tre fallstudier av bristande efterlevnad mera i detalj och några ytterligare i korthet framträder ett likartat mönster. Vissa banker har under flera år varit medvetna, på flera nivåer inom organisationen, om otillräckliga kontroller och accepterandet av högriskkunder. Tillsynsmyndigheterna har också till viss del varit medvetna om bristerna i dessa banker. Likheterna mellan fallstudierna får oss att misstänka att snarlika mönster sannolikt skulle framträda om vi granskade andra fall på djupet, vilket också antyds av uppgörelser mellan regleringsmyndigheter och andra banker.

- Bristande efterlevnad tycks vara ett utbrett problem: nästan alla stora banker i Europa har fått böter, ofta upprepade gånger, för brister eller sanktionsbrott. Det verkar därför ha funnits ett betydande glapp mellan förväntningarna hos tillsynsmyndigheter och bankernas faktiska regelefterlevnad.
- I vissa fall tycks ineffektiv tillsyn och överseende lagföring ha bidragit till långvariga brister i efterlevnaden: tillsynsmyndigheterna var medvetna om bristerna i kontrollerna, bankerna försäkrade myndigheterna om att dessa brister var lösta och myndigheterna avstod från adekvat uppföljning för verifiering.
- Trots det visselblåsarskydd som finns föreskrivet i det tredje penningtvättsdirektivet, med slutdatum för införlivande 15 december 2007, har många anställda med information om allvarliga brister i efterlevnad inte lyckats göra sina chefer uppmärksamma på detta. Eller så har cheferna underlåtit att agera, vilket skulle motivera extern rapportering till tillsynsmyndigheten. Anställda förefaller sakna starka incitament att visselblåsa och de som har gjort det utsätts (som i andra branscher) ibland för repressalier som i sin tur skapar medieberättelser om förstörda liv som sannolikt tjänar till att avskräcka framtida visselblåsare. Vi bedömer att det finns stort utrymme att förstärka visselblåsarincitament för att få till stånd förbättrad tillsyn och efterlevnad av regelverket.

Slutsatser från granskning av regelverket mot penningtvätt

Det globala regelverket mot penningtvätt har utvecklats sedan slutet av 1980-talet, med Arbetsgruppen för finansiella åtgärder, Financial Action Taskforce (FATF), som den primära globala standardsättaren. Det råder delade meningar om regelverkets effektivitet. Kritiker pekar på att endast ett minimum av illegala tillgångar har beslagtagits, att det finns ihållande brister i efterlevnaden, att metoderna för att utvärdera länders insatser är inkonsekventa, att externa effekter som ”de-banking” och ”de-risking” (när banker upphör med sin

verksamhet i högriskområden eller avböjer att ha kunder som de bedömer vara av hög risk) uppstår, att regelverket medför höga byråkratiska kostnader och att det finns en allmän oförmåga att empiriskt mäta effektiviteten i regelverket.

Inom EU har reaktionerna på de senaste penningtvättsskandalerna lett fram till förslag på åtgärder som främst fokuserat på att centralisera tillsynen, förbättra samarbetet mellan medlemsstaterna samt öka tillsynsresurserna.

Slutsatser från granskning av visselblåsarlagstiftning

Under de senaste åren har intresset ökat för att skydda visselblåsare från direkta repressalier och man har runt om i världen tagit initiativ till lagstiftning. Inom EU antogs ett direktiv om visselblåsarskydd 2019, vilket förhoppningsvis förbättrar det nuvarande otillräckliga skydd som finns i många EU-länder.

Förbättrat rättsligt skydd för visselblåsare är ett steg i rätt riktning. Det är emellertid oundvikligen begränsat till de direkta och uppenbara former av repressalier som kan dokumenteras i domstol, men exkluderar många andra indirekta eller fördröjda former av repressalier som en domstol inte kan skilja från vanliga affärsbeslut. Därför är ett kompletterande perspektiv på visselblåsning nödvändigt. Förutom att skydda visselblåsarna som medborgare ska man även se dem som stöd till tillsynsmyndigheterna. Mot bakgrund av den tillgängliga forskningen är det osannolikt att enbart visselblåsarskydd – utan betydande ekonomiska incitament – leder till en effektiv tillsyn och lagföring.

Slutsatser från utvärdering av forskning om belöningssystem för visselblåsare

Oberoende forskning om huvudsakligen amerikanska belöningsprogram för visselblåsare tyder på att väl utformade och rätt hanterade program har flera positiva följder.

- De ökar mängden kvalitativ information om okända efterlevnadsbrister som mottagits av brottsbekämpande myndigheter.
- De har en betydande avskräckande effekt.
- De ger sällan upphov till problem som falska anklagelser och fabricering av bevis eller minskar den interna ”etisk”-moraliska motivationen att rapportera överträdelser (argument som har överdrivits i den politisk debatten).
- De är extremt kostnadseffektiva: studier och administrativa data tyder på att dessa program betalar för sig själva flera gånger om – även om man bortser från deras avskräckande effekter på ytterligare regelbrott.

› De är framgångsrika när de utformas effektivt – till exempel har amerikanska program väsentligt mer bevis till sin fördel än belöningsprogram som införs mot konkurrensbrott, vilka erbjuder visselblåsare lägre belöningssummor.

Rekommendationer för beslutsfattare

› Som svar på de senaste penningtvättsskandalerna har rapporter och rekommendationer från politiker och experter föreslagit olika sätt att centralisera tillsynen på EU-nivå. Centralisering av tillsynen kommer sannolikt att hjälpa till att lösa några av de problem som observerats, till exempel inkonsekvent uppföljning av rekommendationer till banker från lokala tillsynsmyndigheter, otillräckligt informationsutbyte mellan tillsynsmyndigheter samt alltför ”mysiga relationer” mellan lokala tillsynsmyndigheter och reglerade institutioner. Centraliserad tillsyn kommer emellertid inte att väsentligt förbättra den information som tillsynsmyndigheterna får om brister i efterlevnaden och inte heller om adekvata åtgärder har vidtagits som svar på tidigare varningar.
› Oberoende forskning tyder på att detta informationsgap mellan banker och tillsynsmyndigheter kan överbryggas mest effektivt genom att ge visselblåsare ekonomiska incitament. Skyddet för visselblåsare är ofta ofullständigt, eftersom många former av indirekta och uppskjutna repressalier inte kan bevisas i domstol. Belöningsprogram för visselblåsare vid allvarliga fall av bristfällig efterlevnad kan hjälpa till att kompensera för de karriärskador som visselblåsare ofta drabbas av när de rapporterar. För att vara effektiva bör dock sådana belöningsprogram utformas med omsorg och drivas på ett konsekvent sätt av en oberoende myndighet. En lämplig institution skulle kunna vara en centraliserad EU-myndighet.
› Sekretessavtal och klausuler har ofta använts utöver deras avsedda syften, såsom att skydda affärshemligheter, för att avskräcka visselblåsare från att tala med myndigheterna när intern visselblåsning om oegentligheter inte gett några effekter. Sådana avtal bör uttryckligen utesluta förfrågningar från och kommunikation med tillsynsmyndigheter och andra brottsbekämpande myndigheter. Om det inte görs kommer avtalen sannolikt att avskräcka anställda från att förse myndigheter med information – även om de har ett allmänt skydd mot repressalier. Problemet har uppmärksammats av EU-direktivet om visselblåsarskydd. Men sannolikt behövs mer proaktiva åtgärder, till exempel förbud mot sekretessavtal som inte uttryckligen utesluter kommunikation med tillsynsmyndigheter och brottsbekämpande

myndigheter, samt konsekvent sanktionerad användning av dessa sekretessavtal.

› Mot bakgrund av evidens från USA bör FATF, enligt vår uppfattning, betona vikten av att skydda visselblåsare och ge dem ekonomiska incitament. FATF borde i sina utvärderingar vara mer välvilligt inställda gentemot länder som har robusta visselblåsarskydd och incitament att rapportera dålig efterlevnad av penningtvättsregler och som proaktivt sanktionerar otillåtna sekretessavtal, eller att den på andra sätt uppmuntrar länder att anta bättre förfaranden på detta område.

Executive Summary

THE FIGHT AGAINST money laundering became an international priority in 1989, and the first European anti-money laundering (AML) directive was adopted in 1991. Thirty years and four AML directives later, with two more on the way, the problem seems as pertinent as ever: well-known cases like HSBC's AML failures that allegedly enabled drug cartels to launder money for years have in recent years been accompanied by the discovery of AML deficiencies in many other European banks, including some in the Nordic countries.

Financial institutions often remark that the regulatory framework is complex, that procedures for assessing risk and conducting due diligence on risky customers have not been adequately spelled out, and that they are adapting to a continuously moving landscape (six directives is a testament to that). At the same time, European policymakers and experts seem to by and large agree that the current AML supervision has not been sufficiently effective, for example, in terms of assets recovered, and many have called for improving AML supervision and enforcement.

Given the alleged high implementation costs and limited effectiveness of the current AML framework in Europe, new enforcement and supervisory methods should be welcomed. This report is mainly intended to assess the feasibility of one such method recently instituted in this area by the United States: offering financial rewards, funded by fines and recovered assets (undue profits), to whistleblowers who bring particularly valuable information to supervisory or law enforcement agencies regarding severe cases of AML non-compliance. Below are some of the report's central conclusions.

Conclusions from recent cases

Considering select recent cases of AML non-compliance in depth and some in brief, we find that a similar pattern tends to emerge. Certain banks have been aware of inadequate AML controls and the onboarding of high-risk customers at several levels within the organization, often for prolonged periods lasting several years. Supervisory agencies were also to some extent aware of AML deficiencies within these banks. The parallels between the case studies of AML non-compliance we consider lead us to suspect that similar patterns would likely emerge if we considered other cases in depth, which is also suggested by statements drawn from AML settlements with other banks.

- AML non-compliance appears to be a widespread problem: almost all large banks in Europe have been fined, often repeatedly, for AML deficiencies or sanctions violations. There appears, therefore, to have been a significant gap between the expectations of regulators and banks' compliance efforts.
- In some cases, ineffective supervision and lenient enforcement appear to have contributed to prolonged AML non-compliance: supervisors were aware of deficiencies in AML controls, banks reassured them that these deficiencies were solved, and supervisors did not conduct proper follow-up procedures for verification.
- Despite some level of whistleblower protections being mandated in the third AML directive, with a transposition deadline of December 15, 2007, numerous employees with information on serious AML deficiencies did not successfully bring such details to their supervisors' attention (or if they did, supervisors failed to act, which would warrant external reporting to the supervisory agency). Whistleblowers appear under-incentivized and, as in other industries, are sometimes retaliated against—creating media stories of ruined lives that likely serve to deter future whistleblowing. Substantial room remains for improving whistleblower incentives to enhance AML supervision and enforcement.

Conclusions from the survey of AML regulations

The global AML regime has been developing since the late 1980s, with the primary global standard-setter being the Financial Action Taskforce (FATF). Whether this regime is and has been effective is unclear. Critics point to minimal asset recoveries, persistent AML violations, inconsistent methodologies in evaluating countries' AML efforts, externalities such as de-banking and de-risking, the high bureaucratic cost of

the regime, and a general inability to empirically measure its effectiveness, among other issues.

The suggested responses within the EU to the latest money laundering scandals have mainly focused on the centralization of supervision, improved cooperation between member states, and increasing supervisory resources.

Conclusions from the survey of whistleblower legislation

Recent years have seen an increased interest and some legislative initiatives—mainly to enhance the protection of whistleblowers from direct retaliation—in the EU and throughout the world. An EU directive on whistleblower protection was issued in 2019, hopefully improving the currently insufficient protection against straightforward forms of retaliation for whistleblowers who report violations of EU law.

Improved legal protection of whistleblowers is a step in the right direction. However, it is inevitably limited to the direct and evident forms of retaliation that can be documented in court, failing to include the many other indirect or delayed forms of retaliation that a court cannot disentangle from standard business decisions. Consequently, a complementary perspective on whistleblowers seems essential: it is not only necessary to protect them as good citizens but also to think of whistleblowers as persistent monitors and aids to supervisors. In the light of the available research, whistleblower protection alone—without substantial financial incentives—is unlikely to lead to an effective enforcement regime.

Conclusions from the review of research on whistleblower reward programs

Available independent research on (mainly US) whistleblower reward programs suggests that in a variety of regulatory areas, these programs, if well-designed and well-managed:

- Greatly increase the amount of high-quality information on unknown regulatory infringements received by enforcement agencies in the years after their enactment.
- Significantly deters future violations.
- Seldom give rise to problems such as false claims, fabrication of evidence, or the crowding out of intrinsic moral motivation, which have been vastly overstated in policy debates.
- Are extremely cost-effective: studies and administrative data suggest that they pay for themselves multiple times over—even if we ignore their deterrence effects on further violations.

› Result in success when designed effectively. For example, US programs have substantially more evidence in their favor than programs introduced in antitrust enforcement that provide minimal rewards.

Recommendations for policymakers

› In response to recent scandals, reports and recommendations by politicians and experts have suggested different ways of centralizing AML supervision at the EU level. Centralizing supervision is likely to help solve some of the problems that many have observed, such as inconsistent follow-up on recommendations to banks by local supervisors, insufficient information sharing between supervisors, and overly "cozy relationships" between local regulators and regulated entities. However, centralizing supervision is not likely to substantially improve the information the supervisor receives regarding AML non-compliance, nor on whether adequate measures have been taken in response to prior warnings.

› Available independent research strongly suggests that this informational gap between banks and regulators can be most effectively bridged by properly incentivizing whistleblowers. Whistleblower protection is inherently partial, as many forms of indirect and postponed retaliation cannot be proven in court. Whistleblower reward programs for egregious cases of deficient AML practices (and other forms of infringement) may help compensate for the unprotected career damages typically suffered by whistleblowers. However, to be effective, such reward programs should be designed with care and operated in a principled way by an independent agency removed from local political and industry pressures. We believe that a suitable institution to manage such a program could be a centralized EU-wide supervisor.

› Excessively prohibitive non-disclosure agreements can deter whistleblowers from turning to supervisory agencies, even if these agreements are legally unenforceable. These contracts and clauses have often been used beyond their intended purposes, such as protecting lawful trade secrets, to deter whistleblowers from speaking to the authorities when internal whistleblowing on illegal practices produced no effects. Such agreements should explicitly exclude requests by and communication with regulators and other law enforcement agencies. If they do not, these agreements will likely deter employees from providing supervisors with information—even if granted generic protection. While this problem has been recognized by the EU directive on whistleblower protection, more proactive actions are likely

needed, such as banning non-disclosure agreements that do not explicitly exclude communication with regulators or law enforcement agencies and consistently sanctioning their use.

› In the light of the evidence on the US experience, the Financial Action Taskforce should, in our view, emphasize the importance of protecting and incentivizing whistleblowers. It could more favorably evaluate countries that have robust whistleblower protections and incentives with respect to AML and proactively sanction generically prohibitive non-disclosure agreements, or in other ways encourage countries to adopt better procedures in this area.

1. Introduction

THE IMF DEFINES money laundering as "the processing of assets generated by criminal activity to obscure the link between the funds and their illegal origins"; similarly, the Financial Action Task Force (FATF) defines it as "the processing of criminal proceeds to disguise their illegal origin." There is, however, no widely recognized common definition of money laundering (Unger et al. 2006). The term "money laundering" is believed to originate from Al Capone, who used laundromats to obscure the origin of his criminal profits in the 1930s—a time when few had washing machines at home (Unger 2011: 615), making the cash-intensive business a perfect tool to "clean" dirty money.

The World Bank estimates that between 2% and 5% of global GDP is laundered annually. The total world GDP in 2018 was $84.84 trillion, which then suggests that between $1.69 trillion and $4.2 trillion is annually laundered. However, estimates vary considerably, depending on the adopted definition. Simultaneously, it is estimated that less than 1% of proceeds of crime laundered via the financial system are currently seized and frozen by regulatory and law enforcement agencies (UNODC 2011: 7).

Every case of money laundering has what is called a "predicate offense" or "predicate crime" behind it: meaning an illegal act, such as the selling of drugs, smuggling, tax evasion, or human trafficking, that produces profits that need to be laundered in order to be freely used in the international financial system. To curb money laundering, several institutions, including banks, are obligated to adopt preventive procedures to identify customers and transactions that may be involved in or related to money laundering. A primary concern for banks, the institutions on which this report focuses, is having adequate and updated information on their customers and

their activities to prevent being used by criminals looking to launder their money.

Combating money laundering is vital because when uncurbed, it has significant adverse effects on society. Among other things, it enables criminals to enjoy the proceeds of crime, creating a base for further illegal activities; it facilitates government corruption; it makes it possible for dishonest leaders in countries with weak institutions to plunder local resources and developmental aid; it allows tax evasion to undermine fiscal policies, redistribution, and the provision of the most fundamental public goods; it plays an essential role in the funding of terrorist organizations; and it undermines international sanctions. An effective AML regime has the potential to contain these significant problems in societies.

Money laundering can take many forms, with cryptocurrencies playing an increasing role. This report focuses exclusively on AML deficiencies in banks and how to limit them, with particular attention paid to Europe and Scandinavia. The recent cases of failures of AML regimes in the Nordic countries have brought new attention to the topic, spurring a discussion on the effectiveness of the current European AML and Counter-Terrorist Financing (CTF) regime and the possibilities to improve it.

We mainly focus on compliance with the administrative set of rules for institutions covered by AML regulation to prevent or detect money laundering activities, rather than on the criminal side of laundering money and proactive attempts to obscure the criminal origins of funds. This is sometimes called the "preventive" side of money laundering regulation, in contrast to the "repressive" criminal law or "enforcement" side of the fight against money laundering (Reuter and Truman 2004, Svedberg Helgesson and Mörth 2018).

With respect to compliance with the preventive regulation, there is a spectrum of the level of severity of non-compliance. Less serious shortcomings, such as not having adequate staff or competence to ensure AML compliance, have been rather widespread. More serious issues include an extensive lack of knowledge about customers, careless onboarding of high-risk customers, and serving them for extended periods despite repeated internal and external warnings and red flags. Then there are arguably worse offenses, such as employees proactively aiding customers in laundering money, which appears to have been the case at HSBC where employees allegedly aided customers from Iran in avoiding a filter developed by the US Office of Foreign Assets Control to identify and halt potentially prohibited transactions (US Senate 2012).

Whereas customer-facing employees at banks on some occasions have intentionally aided criminals and are therefore guilty of criminal violations, our focus in this report is

primarily on the lack of organizational responses to ensure that rank-and-file employees follow the correct procedures for customer onboarding and scrutinize suspicious transactions, as mandated by AML regulations. Banks are not the only institutions that can enable money laundering, and several other channels exist. However, many banks worldwide have historically been active in this profitable business, and in some "tax haven" countries, it has been their primary activity. Some countries have historically made themselves attractive as custodians of illegally obtained wealth by offering high levels of bank secrecy. Other countries have done so indirectly by allowing for opaque incorporation structures, such as limited liability partnerships, that make it easy for criminals to hide their identity and the origins of their assets.[1]

"Bank secrecy" used to be a neutral or even positive expression in relation to the banking business. While it may have some legitimate purposes, today it often carries a negative connotation and is considered—among other things—an obstacle to tax transparency that undermines governments' ability to collect taxes from the wealthiest part of the population. In recent years, some countries have been effective in detecting and deterring tax evasion and money laundering arrangements. Consider the United States. Many US tax evaders used to hide and launder their undeclared wealth through Swiss banks, but it is widely believed that very few do so today. What happened?

Bradley Birkenfeld, a banker working for the Swiss bank UBS, blew the whistle on how US citizens were evading taxes with the help of his bank. Under US law, persons bringing original information on tax avoidance are eligible for a percentage of the tax collections that their information aids in recovering. Birkenfeld was awarded $104 million for his information on Swiss banking practices; UBS ended up paying a $780 million fine and agreed, together with the Swiss government, to turn over the names of thousands of Americans involved in tax avoidance. The revenues generated by the US government, largely due to Birkenfeld's information, is estimated to be $16.19 billion (KKC 2020), and these whistleblower incentives were intended to and likely succeeded in undermining tax-evading Americans' belief that their money would be safe in Switzerland (see, e.g., Ventry 2014).

Our focus in this report is to understand whether and how whistleblowers can assist supervisors and investigators in the early detection of extensive AML non-compliance within financial institutions by playing a continuous monitoring role.[2] Like many other forms of regulatory violations and white-collar crimes, AML non-compliance has no victims who directly suffer damages, leading to an absence of an injured party with an incentive to report the infringement to the police or

1. Nyreröd and Spagnolo (2021b) consider which countries have enabled the most corporate wrongdoing in Europe and find that if one excludes "specialized" countries like Switzerland and Lichtenstein, the UK and Germany stand out.

2. In this report, we use "whistleblowing" to refer to a person turning to a supervisory agency with information on infringements. Additional types include "internal whistleblowing," when a whistleblower reports concerns within their organization, and what can be called "public external whistleblowing," where the person turns to the media or releases documents publicly.

supervisory authority. Supervisory authorities and law enforcement agencies are at a particularly strong informational disadvantage with respect to these infringements relative to crimes with direct victims, making insider information more important.[3]

Whistleblower reward programs, that provide financial incentives to insiders who report valuable information on infringements to regulators have proven highly effective in uncovering and deterring a wide range of corporate misconduct in the US, remain absent in Europe. On January 1, 2021, the US Congress extended these programs to AML non-compliance, under which whistleblowers would receive up to 30% of the government collections and monetary sanctions imposed on wrongdoing institutions. These rewards only apply to particularly severe misconduct that leads to enforcement actions where the sanction against the wrongdoer exceeds $1 million.

In the US, rewards of millions of dollars to individuals who bring agencies information on infringements are frequently handed out. The Securities and Exchange Commission (SEC) has since 2012 provided more than $738 million in rewards to individuals who reported infringements of financial regulations. Since 2007, the Internal Revenue Service (IRS) has paid out over $1 billion in rewards to whistleblowers revealing conspicuous episodes of tax evasion. The False Claims Act, which rewards those who report fraud against the US government, has a ten-year average of $515 million per year paid to whistleblowers. As we will see when discussing independent research, these programs have increased both the detection and deterrence of the infringements they target, with no burden for the taxpayer.

Whistleblower reward programs can be implemented by any supervisory agency in any regulatory area, while in recent times they have primarily been used in the US. Our focus is on whistleblowers and AML in the European context. That said—whistleblower rewards and effectively incentivizing whistleblowers are relevant to any nation seeking to enhance regulatory compliance. To increase the effectiveness of whistleblowers in detecting AML non-compliance, global organizations with significant "soft power" such as the FATF could develop recommendations in this regard, based on the extensive independent research that emerged in the last decade and is reviewed in this report.

The rest of the report is structured as follows. In Section 2, we consider three cases of AML non-compliance in depth and briefly discuss a few additional incidents. In Section 3, we outline the global AML regime, discussing the increasing criticisms and concerns regarding its effectiveness and the costs for financial institutions. In Section 4, we survey the current state of whistleblower protection and reward laws in the EU

3. "Money laundering is, what the philosopher John Stuart Mill called a 'victimless' crime. It does not produce immediate victims; nobody gets immediately damaged from laundering. The launderer puts his money in a bank, and the bank earns from him opening an account. The launderer buys a house and the real estate agent earns from having the house sold. So, there are no direct negative effects of laundering. Laundering has only indirect effects on society and the economy (when criminals are penetrating the economy and society, the public sector gets hollowed out from lack of tax revenues etc.)." (Unger 2017: 30).

and US. In Section 5, we review the evidence on the effectiveness of whistleblower reward programs, consider some objections against them, and possibilities for using them for AML enforcement in Europe. In Section 6, we conclude with some policy recommendations.

2. Case Studies

MANY EUROPEAN financial institutions, including Deutsche Bank, BNP Paribas, Barclay's Bank, and HSBC, have been fined for AML or sanctions violations in recent years, and several large international banks are recidivists with respect to AML non-compliance. In this report, we focus on recent AML issues within Danske Bank and Swedbank. We also consider a "classic" case, that of HSBC, which is particularly illustrative of the soft stance regulators and governments often adopt with respect to these practices, and at the same time what kind of crimes banks may help enable if they turn a blind eye toward the identity and activities of their customers. In the HSBC case, the bank entered a deferred prosecution agreement over prolonged AML non-compliance that enabled Mexican drug cartels to launder hundreds of millions of dollars through the bank.

It may be challenging to comply with all the rules mandated by the complex AML regulations on any given occasion, so it is probably more appropriate to think of compliance as degrees on a spectrum, with minor violations on one end and severe ones on the other. One could distinguish between: (i) banks complying with the law but unwittingly being used by clever criminals to launder illegal profits while having adequate AML controls; (ii) banks being used by money launderers while having inadequate AML controls or not paying proper attention to red flags (negligence); (iii) banks consciously turning a blind eye to evident and persistent AML deficiencies (intentional negligence); (iv) banks deliberately engaging in typically highly profitable money laundering—proactively helping clients conceal their identity or the origins of their assets. The cases we consider almost exclusively involve AML non-compliance in categories (ii) and (iii), while HSBC is probably more appropriately classified as (iii) and (iv).

In the remainder of this section, we first consider the case of HSBC (Section 2.1), then the recent Scandinavian cases of

Danske Bank (Section 2.2) and Swedbank (Section 2.3). In reviewing these cases, we focus on i) each bank's awareness of AML risks at the group/branch level, ii) the prolonged nature of the offenses while AML deficiencies were known to be present, and iii) communication with and effectiveness of bank supervisors. We end by discussing AML fines against other banks (Section 2.4), how whistleblowers are treated within banks (Section 2.5), and then briefly conclude (Section 2.6). We rely on public sources, including internal investigations by banks, external investigations by supervisors, settlement and sanctions decisions, and complementary information from research and newspapers.

2.1 HSBC

Our first case concerns HSBC Holdings, or "HSBC Group," and its US affiliate HBUS with respect to HSBC's activities in Mexico, a country that has been a member of the FATF since 2000. The section is based primarily on reports from a US Senate investigation from 2012, settlements from US enforcement agencies, and subpoenaed documents from a 2016 report by congressional Republicans (US Senate 2012, DoJ 2012, House of Representatives 2016).

HSBC's activities in Mexico began with the purchase of Bital in 2002. At the time of the acquisition, Bital's compliance functions were reviewed and found to be entirely inadequate. Indeed, the then-head of HSBC Group Compliance noted that "there is no recognizable compliance or money laundering function in Bital at present" (US Senate 2012: 48). After HSBC Group purchased Bital in November 2002, it became HSBC's Mexican affiliate (HBMX). Between 2002 and 2007, HSBC Group began efforts to strengthen the compliance and AML programs.

In May 2004, HBMX's internal auditors filed a report with numerous criticisms of the bank's compliance and AML efforts, finding HBMX's AML function to be operating "Below Standard." In September 2004, the Mexican regulator Comisión Nacional Bancaria y de Valores (CNBV) inspected HBMX's compliance efforts and found them unsatisfactory, contrary to the more positive tone employed by HBMX internally. Later, CNBV fined HBMX more than $75,000 for the AML deficiencies identified in 2004.

In early 2005, an internal HBMX whistleblower hotline disclosed that HBMX compliance officials had fabricated records of mandatory monthly meetings by HBMX's Money Laundering Deterrence Communication and Control Committee and provided the false records to a local CNBV regulator. It was found that the records were fabricated by a junior employee at the direction of the HBMX Money Laundering Deterrence

Director (MLD), who then resigned and left the bank.

In November 2005, during a visit to HBMX by the HSBC Group General Manager of Legal and Compliance, CNBV regulators raised a variety of compliance issues, including the nature of HBMX accounts in the Cayman Islands. Then, in December 2005, an internal audit group produced a report that identified a range of compliance and AML problems at HBMX and rated its compliance "Below Accepted Levels." The audit report was disclosed to HBMX in the spring of 2006, and its finding was widely contested by the then-HBMX MLD Director, who complained to HSBC Group Compliance.

In 2007, HBMX was involved in a public scandal involving a wealthy Chinese Mexican citizen accused of using his Mexican corporations to import, manufacture, and sell chemicals to drug cartels for use in the manufacturing of methamphetamines. The man and his corporations were longtime clients of HBMX and other banks in Mexico. According to HBMX internal documents, the accounts of Unimed (one of the client's firms) were opened by Bital, retained by HBMX, and housed in HBMX's Personal Financial Services division, even though the official clients were corporations and should not have been serviced by this division. Nor were the accounts designated as high risk, despite unusual transactions that had attracted bank attention several times between 2003 and 2007.

In April 2007, the head of internal audits for HSBC Latin America was asked to summarize the AML deficiencies in relation to this scandal: they echoed the identical problems identified five years earlier when HSBC purchased Bital and included "Know Your Customer (KYC) [failures] as identified in branch and continuous audit reports," "The lack of adequate documentation and filing systems which remain from the former Bital days," and "Lack of a compliance culture" (US Senate 2012: 58–59). In October 2007, the Mexican regulator CNBV escalated its efforts and asked to meet with the then-HSBC Mexico CEO to express concerns about HBMX compliance and AML efforts.[4]

Between 2006 and 2009, HSBC Bank USA rated Mexico as "standard risk," its lowest AML category, despite the above-mentioned evidence of serious money laundering risks (DoJ 2012) and several reports on the ongoing situation and risks of the Mexican economy (Naheem 2016: 229). Moreover, from 2007 through 2008, HBMX was the largest exporter of US dollars to HBUS, shipping over $7 billion in two years and outstripping larger Mexican banks and other HSBC affiliates—while US and Mexican authorities repeatedly expressed concerns that these bulk cash shipments could only be this large if they included illegal drug proceeds (US Senate 2012: 4).

In 2008, an HSBC presentation discussed the KYC issues involving Cayman accounts. One slide noted that "almost no progress [had] been made in enhanced KYC completion,"

4. In summarizing the meeting with CNBV, the CEO of HSBC Mexico wrote a letter to the HSBC Group CEO. The letter outlined which steps he told CNBV that HBMX was taking, including new hires and customer file centralizing and imaging, which would give more robust KYC data for anti-money laundering. He also told regulators that HBMX would work on changing the culture of the bank, which would "not happen overnight" (despite these cultural issues having been well-known since the purchase of Bital five years earlier). The letter also states that CNBV officials told the then-CEO that was "what they wanted to hear and they would report back positively" to the head of CNBV (US Senate 2012: 65).

stating that only 25% of files would have complete KYC information by December 2008. At the same time, the head of Group Audit for Latin America and the Caribbean stressed that it was important for the accounts to continue due to the large income they produced (US Senate 2012: 98). That same year, an exit interview with the then-HBMX AML Director was conducted. In the interview, the exiting director "cited a number of examples where despite strong recommendations with the CMP [Compliance] business heads had failed or refused to close accounts or indeed on occasions file SARs [Suspicious Activity Reports]. [The AML Director] thought that there was a culture that [sic] pursuing profit and targets at all costs and in fact had seen no recent improvements in the standard of controls or the types of decisions being taken" (US Senate 2012: 69).[5]

HSBC entered into a deferred prosecution agreement in 2012 and agreed to pay $1.9 billion in fines to US authorities.[6] The deferred prosecution agreement also mandated that HSBC install a monitor to oversee their compliance measures for a five-year period. In the bank's 2017 annual report, the HSBC-appointed monitor concluded that the bank was still not "adequately managing financial crime risk" (HSBC 2017: 78).

To put this case into perspective, it is useful to know that this was not and did not remain an isolated event. Since 2013, HSBC has received fines on another 28 occasions for various forms of infringements in the US (data from violationtracker.org 2020). In 2018, HSBC settled with the DoJ to pay more than $100 million to resolve fraud charges. In 2019, HSBC's Swiss affiliate paid a $192 million fine for helping US citizens to evade taxes. The same year, this affiliate also paid €300 million to settle a Belgian criminal probe into allegations that it helped wealthy clients evade millions of euros in taxes (Sebag 2019).

The 2016 report prepared by congressional Republicans (House of Representatives 2016) contained subpoenaed documents from enforcement agencies and was used by Republicans to argue that the Obama administration was weak on financial crimes during an election year. The report also included documents outlining the involvement of high-level UK political figures. For example, on September 10, 2012, UK Chancellor George Osborne (the UK's chief financial minister) wrote a letter to Federal Reserve Chairman Ben Bernanke (with a copy transmitted to then-Treasury Secretary Timothy Geithner) regarding the HSBC case. In the letter, Chancellor Osborne insinuated that the US government was unfairly targeting UK banks by seeking settlements higher than comparable settlements with US banks. He also expressed concerns related to the effects of possible criminal sanctions against HSBC on financial stability in Europe (e.g., criminal charges could also lead to a revoked license, preventing the bank from conducting business in the US).

5. While HSBC Mexico apparently had systems to flag suspicious transactions, employees were told to disregard red flags (Garrett 2014: 201).

6. The statement of facts from this deferred prosecution concludes that: "From 2006 to 2010, HSBC Bank USA violated the BSA and its implementing regulations. Specifically, HSBC Bank USA ignored the money laundering risks associated with doing business with certain Mexican customers and failed to implement a BSA/AML program that was adequate to monitor suspicious transactions from Mexico. At the same time, Grupo Financiero HSBC, S.A. de C.V. ('HSBC Mexico'), one of HSBC Bank USA's largest Mexican customers, had its own significant AML problems. As a result of these concurrent AML failures, at least $881 million in drug trafficking proceeds, including proceeds of drug trafficking by the Sinaloa Cartel in Mexico and the Norte del Valle Cartel in Colombia, were laundered through HSBC Bank USA without being detected" (DoJ 2012: 3). The report also states that "from the mid-1990s through at least September 2006, HSBC Group Affiliates violated both U.S. and New York State criminal laws by knowingly and willfully moving or permitting to be moved illegally hundreds of millions of dollars through the U.S. financial system on behalf of banks located in Cuba, Iran, Libya, Sudan, and Burma" (DoJ 2012: 18).

2.2 Danske Bank

In the Danske Bank case, over €200 billion of suspicious money belonging to non-resident customers at their Estonian branch is believed to have had been transferred through the bank. The scandal became a major news story, with substantial pressure on the bank and the Danish and Estonian supervisory authorities to explain their inaction. Danske Bank subsequently decided to release a report from an investigation of their Estonian branch. This report, overseen by the law firm Bruun and Hjejle, provides details into Danske's non-resident portfolio in its Estonian branch. However, the report may not be considered fully independent—Bruun and Hjejle is a regular business partner, having been retained several times previously by Danske Bank, and may not be entirely objective (Bjerregaard and Kirchmaier 2019: 22). This section relies on information in the Bruun and Hjejle report but also on a more thorough case study by Bjerregaard and Kirchmaier (2019) and supplementary information from testimonies and newspaper reports.

Danske's Estonian branch resulted from the acquisition of Sampo Pank in 2007, including its Estonian subsidiary AS Sampo Pank, with a portfolio that included customers from Russia and other countries within the Commonwealth of Independent States, like Azerbaijan and Ukraine (Bruun and Hjejle 2018: 3). AS Sampo Pank became Danske Bank's Estonian branch in 2008. This branch had its own IT platform not covered by the same systems and transaction/risk monitoring as Danske Bank group. Further, many documents at the Estonian branch, including information about customers, were written in Estonian or Russian.

The non-resident portfolio had existed since the 1990s at Sampo Pank, and when acquired by Danske in 2007, it held around 3,300 customers. At an Executive Board meeting in early 2010, the Head of International Banking Activities talked about slowly expanding the non-resident portfolio as he had not come across anything that caused him concern. The expansion added around 6,500 customers to the previous 3,300 (Bjerregaard and Kirchmaier 2019: 15–16). In 2013, the non-resident portfolio at Danske's Estonian branch held 44% of the total deposits from non-resident customers in Estonian banks (up from 27% in 2007) and 9% of total deposits from non-resident customers in Baltic banks (up from 5% in 2007; Bruun and Hjejle 2018: 5).

The customers in the non-resident portfolio managed by the separate part of the bank numbered around 10,000, but they were not the only non-resident customers of the branch. An additional 5,000 customers were identified as having "cross-border" characteristics, such as an address or contact data outside of Estonia—putting the total number of

customers subject to investigation at 15,000. The number of incoming and outgoing payments (to recipients outside the non-resident portfolio) received or sent by customers in the non-resident portfolio amounted to approximately 7.5 million for the 10,000 customers. In comparison, for all the suspected 15,000 customers, there were approximately 9.5 million such payments between 2007 and 2015. Funds transferred from external parties to customers in the non-resident portfolio and subsequently transferred from such customers to external recipients amounted to approximately €200 billion for the period 2007 through 2015 (Bruun and Hjejle 2018: 6).

At the time of the release of the Bruun and Hjejle report, 6,200 customers had been investigated out of the total 15,000 non-residents (the first set of investigated customers were prioritized based on scoring high on risk indicators). Almost all these customers were in the non-resident portfolio of 10,000 customers, and only a few of the 6,200 customers investigated have been deemed unsuspicious (Bruun and Hjejle 2018: 32). Bruun and Hjejle conclude that AML procedures for the non-resident portfolio were highly insufficient. With respect to standard due diligence measures, the bank lacked knowledge of the customers, ultimate benefactors, and controlling interests. Customers also included so-called intermediaries, which were unregulated and represented unknown end customers (Bruun and Hjejle 2018: 27). Concerning monitoring of transactions and screening, the report concluded that insufficient attention was paid to customer activities, identification of the source and origin of funds used in transactions was lacking, and there was no screening of customers against lists of politically exposed persons, no screening of incoming payments against sanctions or terror lists, and no automatic screening of incoming payments. In terms of notifying authorities, there was a lack of response to suspicious customers and transactions. Insufficient training of staff and a lack of formal procedures were also identified at the Estonian branch.

It further appears that there were several opportunities for Danske Bank to investigate the issues at the branch and opportunities for the Danish and Estonian financial supervisory authorities (FSAs) to intervene. Bjerregaard and Kirchmaier (2019: 46–50) provide a useful chronology of events that we have shortened and supplemented with the other sources mentioned earlier. Our modified timeline focuses primarily on the interaction between supervisors and the banks and their responses to becoming aware of AML deficiencies.

ACQUISITION OF SAMPO BANK (2006–2008)

On June 8, 2007, the Russian Central Bank shares information with the Danish FSA that clients of Sampo Bank are participating in financial transactions of doubtful origin estimated at billions of rubles per month.

On August 16, 2007, the Estonian FSA issues an inspection report highly critical of Danske Bank's Estonian subsidiary's know your customer procedures and indicates that the bank's routine practice has not complied with legal requirements and international standards, particularly regarding non-resident customers. By December 2007, Danske informed the Estonian FSA that steps had been taken to comply with the orders, including the closure of 597 accounts belonging to non-resident customers.

In April 2008, Group Internal Audit at Danske issues a report on AML procedures in the branch with a "satisfactory" rating (the second-best rating out of five). It also mentions that KYC practices have been improved considerably in the non-resident customer department.

EXPANSION OF THE NON-RESIDENT PORTFOLIO (2009–2013)

In October 2009, the Estonian FSA issues a follow-up AML inspection concluding that Danske has followed the orders from the 2007 precept and that the branch has changed or updated its internal procedures, albeit with some deficiencies.

On March 9, 2010, the Danske Bank Executive Board discusses the number of suspicious activity reports filed by the Estonian branch. The high standard of Danske Bank is mentioned as a reason for the high share of suspicious activity reports compared to other banks in Estonia.

On September 21, 2010, the Danske Bank Executive Board again discusses the number of suspicious activity reports. The Head of Baltic Banking confirms that they are comfortable with the situation in Estonia with substantial Russian deposits. This position is also underlined by the approval received from the Russian Central Bank to establish a representative office in Moscow.

On August 26, 2011, Group Internal Audit issues a report on AML compliance in the Estonian branch with a "satisfactory" rating (the second-best out of five) for compliance and a "fair" rating (the third-best rating out of five) for AML.

On November 14, 2011, the Group Internal Audit releases a report on customer engagement at the Estonian branch, reviewing customer due diligence and procedures with a "satisfactory" rating (the second-best out of five) for the internal control environment.

In January 2012, the Estonian FSA contacts the Danish FSA regarding AML risks in the Estonian branch, noting its grave concern about the extent of non-resident customers at the branch.

On February 20, 2012, the Group Legal and Group Compliance and AML respond to the Danish and Estonian FSA inquiries, writing that they are fully aware that the customer database at Sampo Pank Estonia includes a number of high-

risk customers, but they are confident that the control setup corresponds to the actual risk.

On May 7, 2012, Group Compliance and AML visit the Estonian branch and conclude that some adjustments concerning incoming payment screening and non-resident due diligence are needed. However, the overview of the risk analysis rates all areas in the Estonian branch as green (the best rating out of three) except for two areas rated yellow (the second-best out of three).

On June 15, 2012, the Danish FSA issues nine adjustment orders to Danske Bank on AML following two inspections conducted in 2010 and 2011 on Danish activities alone. Both inspections found several insufficiencies regarding AML procedures. Around the same time, according to Wilkinson (2018), the message sent internally is that the Estonian branch is determined to have the best AML procedures in the group.

On November 30, 2012, the Group Internal Audit issues a report on AML in the Estonian branch with an overall rating of "extensive" (the best rating out of four). The report includes no recommendations for improvement.

In March 2013, the Estonian FSA again approaches the Danish FSA about AML risks in the Estonian branch based on a warning from the Russian Central Bank regarding suspicious Russian customers at the Estonian branch. After investigating, the Estonian FSA concludes that no significant breaches of internal procedures or legal requirements have been found and that while the Estonian FSA remains concerned, there is no reason for immediate regulatory action.

In September 2013, the law firm Brown Rudnick (on behalf of Hermitage Capital) sends extensive documentation to the Danish FSA, the Danish State Prosecutor for Special Economic and International Crime (SØIK), and the Danish Ministry of Justice on the Estonian branch and its use by Russian criminals to launder money. SØIK refuses to investigate the case due to statute of limitations.

CLOSURE OF THE NON-RESIDENT PORTFOLIO (2014–2016)

According to the internal whistleblower reports (Wilkinson 2018):

- On December 27, 2013, Howard Wilkinson (who headed Danske's market trading unit in the Baltics from 2007 to 2014) files the first report, entitled "Whistleblowing disclosure—knowingly dealing with criminals in Estonia Branch," sending it to a member of the Executive Board as well as employees from Baltic Banking, Group Compliance & AML and Group Internal Audit (Bruun and Hjejle 2018: 51).
- His second report, dated January 9, 2014, identifies three UK limited liability partnerships (LLPs), two of which are the most profitable LLPs in Danske Estonia.

- On March 19, 2014, a third report mentions that 12 UK LLPs that are highly profitable for the bank have filed accounts with UK Companies House, and all have registered offices at 175 Drakes Lane, Potters Bar, UK.
- The fourth report, dated April 25, 2014, references Danish K/S companies (limited partnerships equivalent to LLPs).

On January 13, 2014, Group Internal Audit issues a letter confirming some of the whistleblower's allegations. Then, between February 3 and and February 6, 2014, Group Internal Audit conducts an AML audit of the Estonian branch. It concludes by recommending a fully independent review of all non-resident customers.

On February 7, 2014, the Executive Board forms a working group to address the Group Internal Audit findings and recommendations and decides to engage an external consultancy to evaluate internal AML procedures at the Estonian branch.

On March 10, 2014, Group Internal Audit issues a report about the non-resident customers based on the February investigation. The rating used is "Action needed" (the worst rating out of three). One month later, on April 16, 2014, the external consultancy issues a report stating that there had been insufficient knowledge of customers, their beneficial owners, and controlling interests. The screening of customers had been insufficient, and there had been a lack of response to suspicious customers and transactions.

On September 11, 2014, the Estonian FSA issues a draft AML inspection report indicating that the Estonian branch has systematically established business relationships with persons whose activities clearly involve simple and common suspicious circumstances. They also raise concerns that the branch's economic interests seem to prevail over the obligation to apply enhanced due diligence measures.

After this scandal, a disagreement emerged regarding who was primarily responsible for not exercising proper oversight and remedying the issues at Danske Estonia. The Danish FSA argues that the primary AML oversight responsibility for the Estonian branch should be the local FSA (Finanstilsynet 2019), while the Estonian FSA retorts that European rules are not as clear and that the Danish FSA at least has some responsibility to oversee the branches of Danske Group (Finantsinspektsioon 2019).

On September 24, 2018, the European Banking Authority (EBA) opens an investigation to assess whether the Danish and Estonian FSAs have violated any European laws. On April 16, 2019, the EBA votes to reject an internal draft into supervisory failings—a draft that allegedly identifies four breaches of EU law in how Danish and Estonian authorities supervised the bank: "significant shortcomings" in cooperation between Danish and Estonian supervisors, a lack of effective

monitoring of whether the bank has followed due diligence procedures, and insufficient reviews of Danske's governance arrangements (Brunsden 2019). The EBA supervisory board's decision to close the investigation without adopting any findings draws criticism from a range of senior policymakers and spurs calls to reform the supervisory board, which currently consists of senior officials from EU central banks and other banking watchdogs. The EBA has also been criticized for its reluctance to pass judgment on its members (Bjerregaard and Kirchmaier 2019: 38).

Mihhail Murnikov, an employee at Danske's Estonian branch between 2009 and 2015, comments that "the whole non-resident business was built on one principle: Everyone was making money on cross-border transactions because non-residents had to pay $90 per transaction," while Danske's cost for each transaction amounted to only $1. Bonuses were also handed out based solely upon how many transactions employees made; Murnikov states that his strategy was to "make 40,000 transactions a year so that I could get a bonus," and that "you were directly motivated by getting as many clients as possible. Everything else wasn't important" (Reznik and Ummelas 2019). For the year 2013, returns at the non-resident unit hit 402% compared with only 7% for the whole Danske Bank group, which is a clear red flag according to the director of the Danish FSA (Schwartzkopff 2018).

2.3 Swedbank

In February 2019, an investigative report by SVT's Uppdrag granskning alleged that Swedbank had enabled the laundering of hundreds of millions of dollars throughout the last decade, claiming that the money had been moved between suspicious accounts at Danske Bank and Swedbank. The report suggested that at least 50 customers at Swedbank with a clear risk profile and warning signals were able to move around $483 million through the bank (SVT 2019). This section is primarily based on a report by Clifford Chance (2020), investigations by Finansinspektionen, and supplementary material.

In October 2019, the Swedish FSA announced that they were assessing sanctions for Swedbank, and in March 2020, the FSA declared their decision to hand Swedbank a $386 million fine. The investigation considered whether Swedbank had followed the rules on governance and control regarding precautionary measures against money laundering in Estonia, Lithuania, and Latvia from 2015 to the first quarter of 2019. The investigation did not consider whether the Baltic subsidiaries had complied with local (that is, Estonian, Latvian, and Lithuanian) anti-money laundering rules, nor did the investigation evaluate whether money laundering occurred.

The Clifford Chance report concluded that between 2007 and 2016, Swedbank Estonia and Latvia actively pursued high-risk customers as a business strategy. Swedbank also accepted certain customers that had been off-boarded by another bank in Estonia in 2015, which had decided to exit the high-risk non-resident business based on excessive money laundering risk (Clifford Chance 2020: 7).

Similar to how Danske acquired a smaller bank in the Baltics, the smaller Hansabank became a wholly-owned subsidiary of Swedbank in 2005, although Swedbank acquired more than 50% of Hansabank's shares through a share issuance in 1998 (Clifford Chance 2020: 12). As with Danske Bank, there were attempts to separate the high-risk non-resident (HRNR) business from regular information and compliance procedures. Employees at Swedbank Estonia involved in the HRNR business kept a hard copy of certain information regarding the ultimate beneficial owners in a safe or locked drawer to assuage customer concerns that the ultimate beneficial owner may become known to third parties (Clifford Chance 2020: 7).

The report also reviewed transactions using a set of algorithms to determine the portion of transactions at the Baltic subsidiaries that warranted further review. In this analysis, it was determined that across all three Baltic subsidiaries, the total value of the transactions that triggered at least three algorithmic indicators for further review amounted to €17.8 billion of incoming payments, and €18.9 billion of outgoing payments, for the period March 2014 through March 2019 (Clifford Chance 2020: 8).

The report further identified issues regarding communication with regulators. These included Swedbank failing to take an actively transparent posture with regulators regarding AML issues, de-emphasizing negative information, and occasionally employing an overly narrow or literal reading of certain requests (Clifford Chance 2020: 10).

In June 2006, Swedbank Group Internal Audit issued an audit report to managers within Baltic Banking that reviewed AML initiatives in, among other regions, the Baltic subsidiaries. The report noted that "[i]n case of legal persons high-risk nonresidents … in almost all cases it is not possible to verify the real shareholders of companies and/or beneficial owners" (Clifford Chance 2020: 53).

In November 2012, Swedbank Estonia responded to a question by the Estonian FSA about increased payment movements for offshore customers, attributing the increase to a restructuring of the ownership of a group of customers internally known as the High-Risk Customer (HRC-I) Group. Swedbank assured the Estonian FSA that it was aware of and monitoring the reconstruction and transactions and that it had obtained documents from the customer regarding the reconstruction. However, Swedbank Estonia did not in

2012 have sufficient documentation verifying the beneficial owners of the HRC-I Group, an adequate understanding of the legitimate business purpose of the restructuring, nor had Swedbank Estonia adequately implemented risk-based monitoring of the HRC-I Group's transactions (Clifford Chance 2020: 164).

In January 2017, Swedbank responded to a verification letter by the Swedish FSA dated December 23, 2016. The letter identified deficiencies in Swedbank's KYC procedures, stating that "Swedbank has not taken additional measures to reduce the bank's risk exposure to being exploited for money laundering." The response by the bank asserted that Swedbank had "adequate procedures and processes in its operations … a good understanding of the customer, as well as the purpose and type of the business relationship" (Clifford Chance 2020: 165). Then, in June 2017, the head of compliance told an employee that they were not allowed to inform the board about the money laundering risks identified at the Estonian subsidiary (Finansinspektionen 2020a: 34).

The central findings of Finansinspektionen include the following:

- "The investigation shows that Swedbank AB has been aware of suspected money laundering activities in the Baltics. Despite several internal and external reports warning about deficiencies in the Baltic subsidiaries and the risk of money laundering, the bank did not take proper and sufficient action" (Finansinspektionen 2020b).
- "Customers that the subsidiary bank itself classified as high risk have also represented the majority of the volume of non-resident customer transactions" (Finansinspektionen 2020a: 24).[7]
- "… Swedbank withheld and on one occasion provided false information [to Finansinspektionen]" (Finansinspektionen 2020a: 2, 63).

2.4 Other cases

The cases discussed above are samples from a larger pool that reveals how widespread AML problems have been in the banking industry. In 2017, for example, the New York State Department of Financial Services and the UK's Financial Conduct Authority issued fines totaling approximately $660 million to Deutsche Bank for AML non-compliance (DFS 2017). Without considering this instance of non-compliance in depth, it appears to share several characteristics of the cases reviewed in the previous sections:

> Afflicted with inadequate AML control policies, procedures, and structures, Deutsche Bank missed several key oppor-

7. Translations of Swedish texts are our own.

> tunities to identify and interdict this scheme. […] [The violations] occurred at a time Deutsche Bank was on clear notice of numerous deficiencies in its BSA/AML systems and management, and yet the steps it took to remediate the situation proved seriously inadequate. (DFS 2017: 3)

In other recent Swedish cases of AML deficiencies, the bank SEB was fined around $120 million by Finansinspektionen for AML deficiencies and ignoring prior warnings (Finansinspektionen 2020c: 2), and Nordea was given a warning in 2013 regarding AML deficiencies and and was forced to pay a SEK 50 million fine in 2015 (the highest possible fine at the time). Handelsbanken also received a SEK 35 million fine in 2015 for AML deficiencies.

Inadequate AML controls appear to have been common throughout European banking, and Kirschenbaum and Véron (2018: 11) list many other recent fines by European authorities for AML non-compliance. For example, in 2018, the Hungarian National Bank fined MagNet Bank HUF 47 million; in 2017, the Central Bank of Ireland fined the Bank of Ireland €3.1 million; again, in 2017, the UK Financial Conduct Authority (FCA) fined Deutsche Bank £163 million; in 2015, the FCA fined Barclays £72 million for inadequate AML controls related to high-value transactions for politically exposed persons. Since 2016, the US has also issued AML-related fines on eight occasions to banks with headquarters in European countries for an aggregate amount of $1.7 billion (mean $217 million fine; data from violationtracker.org).

The most recent widely publicized AML failure involves Wirecard AG. As a DAX 30 listed company and the "jewel of German fintech," Wirecard AG saw its share price fall from €104 to €2 in nine days after it acknowledged that it could not locate $2 billion that was missing from its accounts. The firm is now apparently under investigation for many infringements, from fraudulent inflation of profits and sales to corruption and money laundering for the bloodiest Mafia organization in southern Italy, the 'Ndrangheta (Johnson and McCrum 2020). According to McCrum and Palma (2019), writing for the *Financial Times*, allegations about these issues go back over a decade: "Accusations of suspect accounting were leveled in 2008, 2015 and 2016. Each time Wirecard has alleged market manipulation, sparking investigations by the German market regulator, BaFin." Nevertheless, the fraud was only officially recognized in 2020, causing substantial losses for investors. Therefore, there was a prolonged period during which the German financial regulator did not act, and in fact, it appears to have acted in defense of Wirecard.

Two recent assessments of the Wirecard debacle, one report commissioned by the European Parliament's ECON committee (Langenbucher et al. 2020) and another by the European

Securities and Markets Authority (ESMA 2020), were critical of BaFin and the supervisory structure in Germany. The ESMA report notes that BaFin believes that there is an extremely high bar for notifying the public prosecutor. However, that seems like an inadequate explanation for not acting in the Wirecard case, as the *Financial Times* published 12 articles on Wirecard in their blog and main paper, containing actionable information, some based on internal documents provided by whistleblowers. Instead of investigating Wirecard, BaFin filed a criminal complaint with the Public Prosecutor's Office in Munich on April 10, 2019 against two journalists on suspicion of market manipulation in relation to their Wirecard reporting (ESMA 2020: 39).

2.5 Whistleblowing in banking

One notable feature of the prolonged and extensive AML non-compliance across the European banking industry documented in this section is the almost complete absence of whistleblowers approaching supervisory agencies. During the extended periods when managers at various levels of the organizations became aware of AML deficiencies, almost no one from these banks reported the severity of these deficiencies to the appropriate regulators or enforcement authorities, or if they did, the supervisory agencies did not initiate the responses required to remedy such infractions.

In banking, however, the lack of whistleblowers is not a new phenomenon—several other instances of prolonged misconduct also suggest that whistleblowers in banking are unlikely to turn to supervisors. A UK Parliament report from 2013 entitled "Changing Banking for Good"—motivated by the poor track record of UK banks concerning risk-taking prior to the financial crisis, the LIBOR scandal, and misselling products to customers—noted the limited role played by whistleblowers:

> One of the most striking features of the series of banking conduct failures has been the absence of whistle-blowing. Ian Taplin noted the extraordinary fact that "there is no public record of any banking employee raising concerns or whistle-blowing" with regards to PPI [Payment Protection Insurance]. The attempted manipulation of LIBOR at Barclays, UBS and RBS was found by the FSA to have continued for a combined total of nearly 20 years, with the direct involvement of 78 individuals in nearly 1,300 documented internal requests and well over 1,000 external requests for alternations to submissions. Much of this manipulation was "deliberate, reckless and frequently blatant." However, no one blew the whistle. (Parliamentary Commission on Banking Standards 2013: 137)

Although we do not know if any employees raised concerns internally in these cases, many cases and studies demonstrate that internal reporting is no guarantee that action will be taken and sometimes ends up with a cover-up or the silencing of the whistleblower. A striking example of this is the 2016 Wells Fargo account fraud scandal, which revealed that the bank had the policy of opening eight accounts per customer and put sales personal under tremendous pressure to achieve that lofty target—leading to the opening of accounts that were unused, unneeded, and unauthorized. It touted this "cross-selling strategy" to investors as key to the bank's financial success. The focus of regulators and the media quickly turned to how top-level management exerted pressure to open as many accounts as possible. Recently, the SEC and DoJ settled with Wells Fargo for a total of $3 billion for misleading investors about the success of this core business strategy.

In an assessment and supervisory self-criticism of the Wells Fargo accounts scandal, the US Office of the Comptroller of the Currency (OCC 2017) concluded that the untimely and ineffective supervision of complaints and whistleblower cases was one of the main issues. Wells Fargo had received a staggering 700 whistleblower complaints related to the gaming of incentive plans. By ignoring these complaints, the OCC concluded, the bank missed several opportunities to perform a comprehensive analysis and take more timely action, beginning in 2010, whereas the fraud became widely known only in late 2016 (OCC 2017: 5).

In the case of Danske Bank, a whistleblower did play a central role in disclosing information and forcing action on the part of the bank, though only very late. In the Wirecard case, external whistleblowing seems to have taken place but was ignored or dismissed by the regulator. Whistleblower information, which served as the basis for some of the *Financial Times* articles on Wirecard, was one of the main reasons the wrongdoing came to light at all (Worth 2020). Later, the identity of the Wirecard whistleblower was revealed to be Pav Gill, who—after pushing for a fraud investigation—was pushed out of the firm and claimed that Wirecard then "tried to destroy me, manfully, professionally, emotionally" (McCrum et al. 2021). Langenbucher et al. (2020: 11) emphasizes the importance of whistleblower information, noting that sources of information at Wirecard did not "receive the attention that (at least ex-post) they should have deserved."

Given such realities, it is unsurprising that whistleblowers in most of the cases discussed have not turned to a regulator with information, despite knowledge of compliance failures for extended periods. Whistleblowers typically suffer severe retaliation of many kinds and are sometimes blacklisted from the industries they work in, and we see no reason to think that this would be different in banking. Retaliation can be quite severe.

Miethe and Rothschild (1994) find, among other things, that among the external whistleblowers they interviewed, 69% lost their job or were forced to retire, 64% were blocked from getting another job in their field, 84% experienced "severe depression or anxiety," and 84% experienced feelings of isolation or powerlessness. The Ethics Resource Center (2014) reports that in 2013, 21% of whistleblowers in the US suffered retaliation, even though whistleblower protection was much stronger in the US than it currently is in Europe.

Not only is the frequency and extent of retaliation documented by several studies, but it is also often accompanied by media stories of ruined lives that will likely make bank employees think twice before going to a supervisor or the public with their information. For example, in 2004, Paul Moore, then Head of Group Regulatory Risk at Halifax Bank of Scotland (HBOS), raised concerns about the bank's risk-taking and was subsequently fired by the executive James Crosby with the argument that "he did not fit in." He was replaced by a person with no risk management experience. Crosby then proceeded to become Deputy Chairman at the Financial Services Authority (FSA), now split into the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA). HBOS collapsed during the financial crisis of 2008 and merged with Lloyds Bank, and many took this to substantiate Moore's claim that the bank had been taking excessive risks. During Prime Minister's question time in the House of Commons, David Cameron commented on then-Prime Minister Gordon Brown's decision to appoint Crosby to the FSA:

> Sir James Crosby, the man who ran HBOS and whom the Prime Minister singled out to regulate our banks and to advise our Government, has resigned over allegations that he sacked the whistleblower who knew that his bank was taking unacceptable risks. (Cited in Dewing and Russell 2016: 165)

In a more recent case in 2018, the CEO of Barclays bank instructed his security team to unveil the identity of a whistleblower who anonymously authored a letter containing concerns about a longtime associate of the bank—despite being warned by compliance staff against taking retaliatory action. He received a fine of £642,000 and was ordered to repay a bonus of £500,000—a sanction many believed to be lenient, sending a clear message on banking regulators' stance to future potential whistleblowers.

In additional cases, Wells Fargo paid a fine of $575,000 and was ordered to reinstate a whistleblower who had complained about the accounts in the scandal mentioned above and was subsequently fired. Deutsche Bank appears to have fired several whistleblowers throughout the years, only a few of

whom have been vindicated (see, e.g., Colapinto 2016). Many other examples of mistreatment of whistleblowers and a lack of response to whistleblower complaints within the banking industry have been reported in the news in recent years (see, e.g., Robinson 2019, Worthington and Christodoulou 2020).

2.6 Conclusions

To put the case studies in the prior section into context, it is important to understand the structure banks have in place to ensure AML compliance. This model is called the "three lines of defense model," and it appears from our case studies that all lines have failed to varying degrees. The first line of defense is managing own risks and is responsible for maintaining effective internal controls, including identifying, assessing, and mitigating risks, often facing customers on a regular basis. The second line of defense is compliance functions and risk management. These functions or committees monitor non-compliance risks at the first line of defense. In the case of banking and AML, there is often an AML compliance function that serves this purpose. The third line of defense is the internal audit function, which is independent and is supposed to provide the board or governing body, as well as senior management, with assurances of compliance with laws and regulations, outlining how the first and second lines of defense achieve these compliance objectives.

With respect to the first line of defense, Danske Bank Estonia, for example, reported 42 employees and agents to the Estonian FIU who were deemed to have been involved in suspicious activity, and ten were arrested by the Estonian state prosecutor (Reuters 2018). At HSBC, employees aided customers from Iran to avoid a filter developed by the US Office of Foreign Assets Control to identify and halt potentially prohibited transactions, including from Iran (US Senate 2012). HSBC Mexico for some period only had adequate information on 25% of its customers. Employees at Swedbank Estonia involved in the HRNR business kept a hard copy of certain information regarding the ultimate beneficial owners in a safe or locked drawer to assuage customer concerns that the true ultimate beneficial owner might become known to third parties (Clifford Chance 2020: 7).

The second and third lines of defense intended to identify and remedy these compliance issues also often failed to do so. At Danske, the internal audit function had rated the Estonian branch as "fair" in 2011, whereas in 2014, it was discovered that it was full of compliance failures. At Swedbank, all lines of defense appear to have informed the board of insufficient resources and competence regarding AML, yet they remained under-resourced and lacked the necessary competence for

years (Finansinspektionen 2021a). At HSBC, a compliance manager had fabricated records of meetings and provided them to the local regulator. Employees at all three lines of defense within these banks would, in our opinion, have been justified in turning to the supervisor with information, especially after years of little to no action on the part of the banks.

Then there is what can be called the "external" or "fourth" line of defense, which is the supervisor and other enforcement agencies. Several problematic features are also noted in the following sections about this line of defense.

Our review of the case studies and complementary reports and material suggests that AML deficiencies of various degrees appear widespread within banking in Europe, given that many large European banks appear to have been fined for various forms of AML non-compliance, some of them being recidivists. Some of the banks we considered observed an abundance of internal warning signs for extended periods, had been warned several times by supervisors, and yet did not rectify their AML compliance problems. Worse, on some occasions, banks or bank employees fabricated documents, interpreted information requests narrowly, and omitted important information, making the supervisor's job more difficult.

Overall, supervisors appeared to be rather ineffective in making banks remedy their problems. Our case studies suggest that supervisors were aware of AML weaknesses in the banks and frequently issued warnings, but then accepted banks' assurances that they had improved without conducting adequate follow-up or verification. A review of banking supervisors by the European Banking Authority reached a similar conclusion: "In several cases, banks continued to be in breach of the same legal provision many years after a fine had first been imposed but were not challenged by the respective competent authority" (EBA 2020: 18).

Under Article 27 of the third AML directive, whistleblowers should have been protected since December 15, 2007, the deadline of the transposition. If there were whistleblowers to supervisory agencies in the three cases we considered, their information was not acted upon. We believe that a more likely conclusion is that there were very few to no whistleblowers who provided valuable information on the onboarding of high-risk customers to the supervisors in the case of Swedbank and Danske Bank. In the Danske Bank case, a whistleblower was instrumental in uncovering the non-compliance issues, although only after several years of other employees not doing so. All this suggests ample room to improve whistleblower incentives to aid in AML supervision and enforcement.

3. Overview and History of AML Regulations

HOW DID WE END UP in a situation in which several large banks do not comply with regulations for extended periods of time? What are the regulatory expectations of banks, and how did they come about? How have policymakers responded to these recent AML failures? We try to answer some of these questions in this section. We begin by briefly reviewing the evolution of AML regulations, starting with efforts at the global level through the FATF (Section 3.1), then examine the European AML context (Section 3.2), and then outline AML developments in Sweden (Section 3.3). Some criticism of the global AML regime is considered in Section 3.4, its foreseeable future evolution in Section 3.5, and in Section 3.6, we provide a brief conclusion.

3.1 FATF and the risk-based approach

The global fight against money laundering initially focused on drugs and drug trafficking—with the 1988 Vienna Convention[8] that prohibited the laundering of drug proceeds (although it did not use the term "money laundering"). The same year, principles on dealing with money laundering were adopted by the Basel Committee on Banking Supervision (consisting of banking supervisory authorities from several states), and in 1989 the Financial Action Task Force (FATF) was formed by the G7—largely due to US initiative (Unger 2017: 11). The Strasbourg Convention[9] in 1990 is the first multilateral treaty to deal generally with "laundering offenses," also widening the scope of predicate offenses beyond drug trafficking (Bergström 2018: 35).

One of the most critical institutions in the context of money laundering internationally is the FATF, which sets the international standards on combating money laundering and the

8. United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances.

9. The Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.

financing of terrorism. It is an independent inter-governmental body that develops and promotes policies to protect the global financial system through AML and CTF recommendations. FATF issued its first set of recommendations in 1990 to combat the misuse of financial systems by persons laundering drug money. Throughout the years, FATF has revised its recommendations: in 1996, it broadened the scope well beyond drug money laundering, and in 2001 it proposed eight special recommendations to prevent terrorist financing. The recommendations were revised again in 2003, and most recently in 2012, and have since been continually updated, most recently in June 2021 (FATF 2021: 7). The decision-making body is called the FATF Plenary, which meets three times per year, evaluates countries that have applied for membership, and monitors the implementation of the applicant countries' action plans against money laundering and terrorist financing.

The current recommendations set out essential measures that countries should have in place to identify risks, develop policies and domestic coordination among competent authorities, apply preventive measures for the financial and other sectors, establish powers and responsibilities for competent authorities, enhance the transparency and availability of beneficial ownership information of legal persons and arrangements, and facilitate international cooperation (FATF 2021: 7). The FATF recommendations—or "soft laws"—have been endorsed by over 180 countries and incorporated into the EU AML directives and US law. While the FATF recommendations remain a soft law instrument, they have obtained a quasi-binding character. The sanctions and costs of non-compliance include the risk of exclusion from the FATF and subsequent adverse consequences, such as an inability to participate in international forums like the Financial Stability Board. FATF also has a blacklist of high-risk and non-cooperative jurisdictions, and FATF members are encouraged to severely restrict or fully prohibit transactions with financial institutions from blacklisted jurisdictions (Gadinis 2015: 31).

What characterized AML efforts in its early days was a "rule-based" approach, which stipulated certain rules that should be abided by (e.g., submit a suspicious transaction report for every transaction that exceeds €10,000). Since 2003, however, there has been an international convergence toward a "risk-based" approach, which instead focuses on identifying risky areas or sectors and allocating resources and enforcement efforts according to risk. The promise of a risk-based framework is that it would reduce compliance costs for the private sector but also ensure that the highest ML/TF risks receive the greatest attention in terms of resources (Borlini and Montanaro 2017: 1020). The idea behind a risk-based system is that it allows obliged entities a relatively cheap and straightforward ordinary procedure for retail banking and cases that

pose little risk in general. As the level of risk increases for a customer, obliged entities fall under more obligations such as determining the source of wealth, its possible destination, and the economic rationale of a given transaction (Borlini and Montanaro 2017: 1040).

The risk-based approach was first developed by the Financial Services Authority in the UK around the year 2000 (Fan 2017, Sergeant 2002) and has for a long time been associated with the insurance industry (Duyne et al. 2018: 346). This approach would shape AML legislation for the future, and in 2012 the FATF expanded upon and adopted risk-based AML principles.

The FATF utilizes mutual evaluation reports (MERs) to screen compliance with its recommendations among its members. MERs are peer evaluations of FATF members, and their purpose is to assess the level of implementation of the FATF recommendations in the member state. The basis for MER reports is provided in an extensive 182-page FATF document on the methodology of these reports, which has been criticized for a number of issues such as a lack of consistency in evaluations between countries (see, e.g., Duyne et al. 2018: 355–365).

Members of the FATF should also carry out their own "national risk assessments," which are intended to demonstrate a member state's self-awareness of risks and vulnerabilities. They should be used to (a) improve its AML/CFT regime, in particular by identifying any areas where obliged entities are to apply enhanced measures and, where appropriate, specifying the measures to be taken; (b) pinpoint, where appropriate, sectors or areas of lower or greater risk of money laundering and terrorist financing; (c) use this knowledge in the allocation and prioritization of resources to combat money laundering and terrorist financing; (d) use it to ensure that appropriate rules are drawn up for each sector or area, in accordance with the risks of money laundering and terrorist financing; (e) promptly make appropriate information available to obliged entities to facilitate outside assessments of money laundering and terrorist financing risks.

The FATF recommendations serve as the basis of AML efforts globally, and most of them are incorporated into the legal frameworks in the US and EU, while in some cases, the FATF recommendations go further than current regulations.

3.2 European AML/CTF directives

The first European AML directive (1991/308/EEC) from 1991 responded to FATF's original 40 recommendations of 1990, the 1988 UN Vienna Convention, and the Council of Europe Strasbourg convention of 1990. The 1991 directive covered the prohibition of money laundering by reference to "criminal

activities," which at the time mostly covered drug offenses. Importantly, the directive set out rules for member states, such as identifying beneficiaries or customers when entering a business relationship, for transactions exceeding €15,000, and otherwise suspicious transactions.

All identification documents, evidence, and records that have been collected for due diligence must be kept for at least five years by financial institutions. The second EU AML directive (2001/97/EC) from 2001 expanded the scope of covered entities to include legal professionals, insurance companies, remittance offices, and casinos.

The third AML directive (2005/60/EC) from 2005, with a transposition deadline on December 15, 2007, extended and strengthened the EU's AML framework. Upon the transposition deadline, it applied to both Swedbank and Danske Bank and their subsidiaries, entailing that the host nations should have implemented national laws requiring banks to have risk-based controls, policies, and procedures in place to detect and deter money laundering. Whereas the first directive imposed customer identification requirements, it contained few details on how to conduct such procedures, which was spelled out in the third directive.

Central to the third AML directive was the demand for customer due diligence, which mandated the identification and verification of customers and their identity based on information obtained from a reliable and independent source and conducting ongoing monitoring of transactions in the business to ensure consistency with the expectations of that particular field. It also required identifying beneficial owners on some occasions and taking adequate measures based on the risk level to verify their identity. There are four measures that institutions covered by the AML directive should do and know with respect to their customer: identify the customer and verify the customer's identity, know and assess the nature and purpose of the business relationship, identify the customer's beneficial owner, and keep the information up-to-date (Forsman 2020).

In certain high-risk situations, it could be necessary to conduct "enhanced due diligence," and it is sometimes also explicitly required—such as when dealing with politically exposed persons and for customers who were not physically present to be identified. The directive further required that rules for record-keeping, customer due diligence, risk assessment, and management be established. Article 27 recognized the need to protect employees who report suspicions of money laundering:

> Member States shall take all appropriate measures in order to protect employees of the institutions or persons covered by this Directive who report suspicions of money laun-

> dering or terrorist financing either internally or to the FIU [Financial Intelligence Unit] from being exposed to threats or hostile action. (2005/60/EC: 28)

The fourth AML directive (EU 2015/849) from 2015, with a transposition deadline of December 16, 2017, enhanced the risk-based approach to monitoring and customer due diligence to align the EU framework with FATF's recommendations. Article 38 of the fourth AML directive further specifies that employees should be protected from employment retaliation:

> Member States shall ensure that individuals, including employees and representatives of the obliged entity, who report suspicions of money laundering or terrorist financing internally or to the FIU, are protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions. (EU 2015/849: 99)

The Swedish government considered this article satisfied following its adoption of the Swedish whistleblower protection law (Regeringen 2017: 347), which came into effect January 1, 2017 (see section 4.1.1).

The fifth AML directive (EU 2018/843) from 2018, with a transposition deadline of January 10, 2020, was primarily a response to the revelations of the Panama Papers, when 11.5 million documents from the Panamanian law firm Mossack Fonseca were released by a whistleblower using the pseudonym "John Doe," who appears to have acted for social reasons and claimed that he wanted to "make these crimes public." This fifth AML directive improved the work of financial intelligence units by providing them with better access to information through centralized bank registers. This directive further enhanced transparency by setting up publicly available beneficial ownership registers, tackling terrorist finance risks in the virtual currencies and pre-paid instruments, and broadening the criteria for assessing high-risk third countries.

The sixth AML directive (EU 2018/1673), also from 2018, with a transposition deadline of December 3, 2020, harmonizes the definition of a "predicate crime" and provides a list of 22 predicate crimes that all EU member states must criminalize, including tax and environmental crimes. The directive also aims to increase cooperation and introduces rules to help determine which country has jurisdiction when a violation occurs in more than one member state.

3.3 Recent AML/CTF developments in Sweden

Sweden carried out a national risk assessment of money laundering and terrorist financing in 2019, which highlighted four problematic themes:

- Front men and misused identities are used in money laundering schemes. Two risk factors within the Swedish system are trust in basic identification and insufficient opportunities for certain authorities to protect themselves from being used for illicit purposes.
- Increased access to and dissemination of information and knowledge is a key condition for an effective Swedish regime against money laundering and terrorist financing. Information must be shared both between authorities and between authorities and operators.
- In certain areas, there are not enough resources, tools and legislation for the coordination function to take proper action against money laundering and terrorist financing.
- The Swedish regime needs to increase its capability to detect and tackle complex, large-scale money laundering schemes. (Swedish National Risk Assessment 2019: 5)

Sweden has seen an increase in the submission of suspicious activity and transaction reports. In 2014, Finanspolisen received a total of 9,183 reports; in 2015, the number was 10,170; in 2016, it grew to 13,322; in 2017, it reached 16,551; in 2018, it again increased to 19,306; in 2019, it was 21,695; and in 2020, it rose to 24,505 (Finanspolisen 2021). In 2018, three categories of suspicious transactions made up 64.6% of the total number of reports. These were repeated or large transactions to an account (28.2%), unusual or deviating transactions (20.3%), and terrorist financing (16.1%).

A report by BRÅ from 2019 suggests that current AML efforts may not have been successful with respect to catching multi-criminals:

> Cases that do not contain a known predicate offense are often complex and resource demanding, have an uncertain conclusion, and demand extensive financial investigations. […] This gives a picture of the difficulties of proving a money laundering offense in cases that are not connected to fraud. This, in turn, indicates that the lawmaker's intention to convict multi-criminals that have amassed proceeds of crime over a period of time has not been successful in a wider meaning. (BRÅ 2019: 9)

As in many other countries, Swedish banks have raised concerns that AML compliance is costly and imposes burdens on

bank customers. A former Swedish regulator who stopped working in 2015 commented that:

> I had discussions with senior bankers in board rooms of major banks in this country where it all was about, basically, me forcing them to harass their customers, and I think that mentality hasn't been helpful at all in the banking sector. It hasn't been to stop money laundering; it hasn't been about stopping or making it more difficult to do criminal activity. It's about regulators forcing us to build up a compliance machine that is inherently something bad for our business because it makes our customers annoyed with us. (SNS 2019)

In 2017, FATF published the fourth-round mutual evaluation report on AML and CTF measures in Sweden. They concluded that Sweden has a reasonable understanding of ML/TF risks, but that this is inconsistent across authorities. According to the report, before the new ML offense was introduced in 2014 and the new TF offense was introduced in 2016, Sweden suffered problems with both offenses. The report concluded that:

> Sweden prioritizes international cooperation and has established highly effective mechanisms for providing it, including specific liaison mechanisms with Nordic and Baltic neighbors, EU cooperation instruments, and dedicated channels for operational cooperation with law enforcement authorities. (FATF 2017: 3)

The government decided to increase Finansinspektionen's money laundering supervision resources by SEK 10 million in the 2020 budget (Finansinspektionen 2019: 3), and resources have been reallocated to AML supervision with the number of specialists on the issue increasing from 7 to 13 (Finansinspektionen 2019: 20). A Baltic working group has also been established, including financial supervisors from Denmark, Estonia, Finland, Latvia, Iceland, Lithuania, Sweden, and Norway.

3.4 The effectiveness of the current AML/CTF regime

We now turn to concerns and assessments of the effectiveness of the global AML regime outlined in sections 3.2 and 3.1.[10] How do we measure the effectiveness of the current regime? There are two measures of effectiveness that have been used in this context. The first is formal compliance and program implementation (Halliday et al. 2019: 8), and in this regard,

10. By the "AML regime," we refer to the global standards developed by the FATF and their implementation in national law—which, although not completely symmetric across jurisdictions, are sufficiently similar to be considered a regulatory regime.

the FATF appears to be largely successful. While lacking any legal standing internationally, the FATF has managed to achieve broad compliance among member states with its recommendations. With respect to this aim, the current regime has been effective: in practice, most FATF members do comply with its recommendations.

The second measure is more ambitious and similar to economic policy evaluations, considering "program effectiveness" or "outcome effectiveness." The focus is on the actual outcomes and comparative benefits, asking questions such as to what extent does the present AML regime deter predicate offenses? Does it succeed in preventing the financing of terrorism? Does it recover a significant portion of laundered money? Is the AML regime proportional to the problem? Does the current AML regime have significant negative externalities? Is it justifiable from a cost-benefit perspective? With respect to several of these questions, many scholars and policy experts have regarded the current global AML regime as ineffective in several respects (Duyne et al. 2018, Halliday et al. 2019, Kirschenbaum and Véron 2018, Pol 2018, 2020). Below, we highlight some of the central objections and concerns that have been raised against the current regime.

3.4.1 COSTS FOR GOVERNMENTS AND ENFORCEMENT AUTHORITIES

The procedure of FATF's membership evaluation reports is to send several investigators to evaluate a country's compliance with FATF recommendations. These reports frequently exceed 200 pages and are jointly carried out by at least three experts, but in most cases, many more. For Italy and Spain, it took 16 days of on-site visits by eight and ten evaluators, respectively, to complete the MERs (Duyne et al. 2018: 359). Forsman (2020: 30) also describes some costs that are less publicly assessable, describing that for Sweden's MER, published in 2017: "Merely to enable the assessment of technical compliance, Swedish authorities wrote a 334-page document that was submitted to the FATF together with hundreds of translations of acts, ordinances, instructions, strategies, process descriptions, decisions, written communications, brochures and so on."

An AML consultant and former co-chair of the FATF Evaluation and Compliance Group recently commented that he is far from convinced that the current Membership Evaluation Reports are picking up on effectiveness:

> This [Membership Evaluation Reports] has become a real spawning ground for consultancy. I am very concerned about the quality of some of the consultancy and the sheer cost to jurisdictions of going through this process, and the cost of the FATF and membership of the FATF—it is phe-

> nomenally expensive [...] I am not really sure it is delivering value for money. (RUSI 2019)

Then there is the administrative cost of screening suspicious activity and transaction reports. Sir Rob Wainwright, former head of Europol, remarked that "95% of suspicious activity reports sent to the FIUs are junk" (SNS 2019). Another report that included interviews with past and present heads of financial intelligence units concluded that 80–90% of suspicious reporting is of no immediate value to active law enforcement investigations (Maxwell and Artingstall 2017). However, progress is being made in this field with increased knowledge and more systemized reporting.

3.4.2 COSTS FOR FINANCIAL INSTITUTIONS AND COVERED ENTITIES

The current regime is widely regarded as being costly for covered entities to comply with. There have been several attempts at assessing the cost of AML compliance using different methodologies.

In a survey report from September 2017, LexisNexis (2017) considers the annual AML compliance cost in five European countries (France, Germany, Italy, Switzerland, and the Netherlands). The report states that the annual cost of AML compliance in these countries totaled $83.5 billion (LexisNexis 2017: 4), with German compliance cost being by far the greatest, at $46.4 billion annually. The report also finds that KYC programs and AML compliance management constituted 71% of the costs (9).[11]

As for North America, another LexisNexis (2019) survey report concludes that the projected cost of AML compliance across all US and Canadian financial services firms totaled $31.5 billion, with US financial institutions accounting for $26.4 billion and Canadian institutions $5.1 billion (4).[12] The report also finds that KYC programs and AML compliance management constituted 51% of costs in the US and 48% in Canada.

Of course, these survey data should be considered with caution. The methodology is not always rigorous and consistent (it is striking that the estimate for Germany is almost twice as large as the US, while the US economy and financial sector are significantly larger than the German ones).

As for the UK, the British Bankers' Association estimates that its members are spending at least £5bn annually on core financial crime compliance, including enhanced systems and controls and staff recruitment (Artingstall et al. 2016: 14).

Magnusson (2009) estimated that Swedish banks spend SEK 400 million annually—based on data from 2005 and 2006.

Compliance Week (2015: 12) approximates that in the two to three years after their 2015 report, financial institutions

11. Their methodology involved conducting surveys by phone, with a total of 250 surveys completed for the five nations. They then extrapolated from these surveys to all financial institutions across the five study markets (LexisNexis 2017: 30).

12. Their methodology involved conducting surveys by phone, with a total of 143 completions (117 US, 26 Canada). We assume that they extrapolate from this data, as in the 2017 report.

globally would be spending more than $10 billion for AML compliance controls.

These estimates vary widely, and it is beyond the scope of this report to conduct an independent analysis of the costs to financial institutions. However, simply comparing these estimates and relating them to any measure of a country's financial sector reveals that each study must be using different methodologies and, therefore, some central guidance is needed on how to perform these estimates.

3.4.3 ASSET RECOVERY RATES

What proportion of laundered money is recovered? A study from the United Nations Office on Drugs and Crime concludes:

> The results also suggest that the "interception rate" for anti-money-laundering efforts at the global level remains low. Globally, it appears that much less than 1% (probably around 0.2%) of the proceeds of crime laundered via the financial system are seized and frozen. (UNODC 2011: 7)

This low rate has been a concern of many regulators and academics, as high asset recovery rates would do the most damage to a criminal's bottom line and potentially deter some predicate offenses.

3.4.4 THE MULTITUDE OF WAYS TO LAUNDER MONEY

While the present study focuses on banks, a pertinent issue for money laundering remains that the methods are diverse and constantly changing. Instant money transfer applications have been used to launder money, as well as gaming platforms such as Steam. Bitcoin and other cryptocurrencies and assets have also been an area of recent regulatory emphasis. Unger (2017: 16–21) provides an extensive list of some of the different ways in which money is laundered. The history of the AML regulation is partly that of successively expanding the scope of the law to cover more and more sectors: from casinos to antique shops, and now cryptocurrencies. In the latest Action Plan on AML by the European Commission, they make it clear that the scope of obliged entities will likely have to be extended (European Commission 2020: 6).

The multitude of ways in which money is laundered makes it hard for regulation to remain effective and adapt to new circumstances. While the current regulatory regime may be proportionate to the way money is currently laundered, new laundering methods may cause redundancies, and the issue of keeping up the cat-and-mouse game may constitute an inherent problem in the rather slow regulatory processes. For example, the process from considering a new directive to its

acceptance at the EU level takes at least one year. Member states are then given two years to transpose the directive.[13]

3.4.5 DE-BANKING AND DE-RISKING

A consequence of the current regulatory regime is the phenomenon of de-banking and de-risking, when banks stop operating in high-risk areas or decide to abandon what they consider high-risk customers. While this may, on some occasions, prevent money laundering, it has resulted in many non-laundering persons and organizations being let go because of the perceived risk they pose. Many banks now want to rid themselves of businesses that might expose them to AML/CTF sanctions. In some cases, charities have had their bank accounts closed without evidence of wrongdoing (Levi 2018: 275).

De-risking can frustrate AML/CFT objectives as it pushes higher-risk transactions out of the regulated system into more opaque and informal channels that are harder to monitor (Silva 2019: 66). Ramachandran et al. (2018) explore some further effects of the current AML regime with respect to de-banking and de-risking. They document how, concerning remittances, several international banks have closed their relationships with money transfer operators in regions they deemed to be too high risk. Among those most likely affected by this broad-brushed closure of accounts are families of migrant workers and small businesses.

3.4.6 LACK OF STUDIES DOCUMENTING PROGRAM EFFECTIVENESS

Given the high costs, low asset recovery rates, and de-banking and de-risking of the AML regime, we could not find studies that have succeeded in estimating the benefits or effectiveness of the global AML regime. As we mentioned, many observers are skeptical of its effectiveness (Halliday et al. 2014, Levi et al. 2018, Pol 2020). Without a well-designed policy evaluation effort, it is hard to dismiss such criticism. Criminals may therefore face minor marginal costs in avoiding the current AML regime, while the societal costs of complying with it may far surpass its benefits.

3.5 The future of AML in the EU

The previous sections have discussed the history of AML/CFT, concluding with some criticism and concerns surrounding the effectiveness of the current regime. However, policymakers in the EU have reacted quickly to new scandals, and several proposals for improvement have been suggested. The US is also moving forward with improving its AML/CFT regime.

Current discussions in the EU concern how to supervise

13. Maximilian and Teichmann (2020) provide qualitative empirical evidence from surveys with illegal financial service providers and find that AML and CTF mechanisms can be easily circumvented. The evidence suggests that compliance officers are aware of money laundering in certain sectors, but not in others—consultancy firm schemes are particularly hard to detect.

banks more effectively in the future. For example, the finance ministers of France, Germany, Italy, Latvia, the Netherlands, and Spain issued a joint position paper arguing for a European supervisory mechanism for ML/FT (JPP 2019) that should focus on particularly at-risk institutions and intervene when national competencies are inadequate. The position paper also suggests that industry influence on national supervisors (i.e., capture) is a problem that would not be as pronounced with an EU-wide supervisor.

A recent report by a senior expert on money laundering (Unger 2020) stresses the need for a European supervisory body and suggests that the European Public Prosecutors Office, whose responsibility currently concerns financial crimes against the EU budget, could have its responsibilities expanded. This European supervisor "should be an autonomous body, sufficiently staffed, and have direct powers of sanctioning. Supervision should concern all financial institutions. Non-financial institutions should be excluded, since they are too diverse" (Unger 2020: 13).

Kirschenbaum and Véron (2020) also argue that a new EU agency is needed and that it should have a direct AML supervision mandate, as the role of "supervisor of supervisors" acts too late. They further contend that the AML supervisor should be authoritative, independent, and able to impose fines and business restrictions on non-compliant firms. Both Kirschenbaum and Véron (2020) and JPP (2019) argue that AML harmonization should take the form of an AML regulation and modification to existing directives.

Lastly, there is the European Commission Action Plan on AML. In the Commission's 2020 Action Plan on Money Laundering, one of its six pillars is "Bringing about EU level AML/CFT supervision," which reads:

> The need to ensure high-quality supervision in cross-border cases and to avoid weak links in the EU supervisory framework provide compelling reasons for an EU body to be entrusted with direct AML/CFT supervisory tasks over certain obliged entities for which it could have exclusive or joint responsibility. This implies the ability to review the internal policies, procedures and controls as well as their effective implementation by supervised entities, along with reviewing documentation on transactions and customers. The Union supervisor could be tasked, on its own or jointly with the national supervisor, with carrying out supervision of clearly defined obliged entities or types of activities for a given period of time, based on the degree of risk posed. (European Commission 2020: 8)

Hence, the policy developments in the EU appear to drift toward increased centralization, either through a new insti-

tution or an expanded mandate to a present institution such as the European Banking Authority.

3.6 Conclusions

In this section, we reviewed the global AML regime and focused specifically on the European directives, the future of supervision in the EU, and the effectiveness of the current AML regime. It is hard to assess the success of the current global regime: the critics are many, and we lack counterfactuals for how things would have looked without the FATF and the global regime. Available estimates of asset recovery rates are also so low that many argue they are unlikely to deter anybody from engaging in crimes that generate money that must be laundered. The regime is also costly—which should warrant accountability in terms of proven enforcement benefits.

Based on the review in sections 2 and 3, it is hard to disagree with Kirschenbaum and Véron's (2018: 4) assessment that "AML supervision in the European Union has been embarrassingly ineffective and that deep reform is needed." In recent years, the idea of centralizing parts of AML supervision at the European level appears to be the central policy direction going forward. In the next sections, we review how enabling and incentivizing whistleblowers can aid in improving supervision.

4. Survey of Whistleblower Legislation

WHISTLEBLOWER PRACTICES AND LAWS have a rich history, which is far beyond the scope of this report to describe. We instead focus on the most recent developments in Europe and the US. We can distinguish two kinds of whistleblower regimes: a "protection regime" that protects whistleblowers from employment-related retaliation and a "reward regime" that also offers whistleblowers monetary rewards for their information. More emphasis will be placed on reward programs for whistleblowers, as protections are already underway with a new EU directive, the more general point of enhancing AML laws through whistleblowing has been made elsewhere (Yeoh 2014), and research as well as agency experience favor reward programs over mere protections. In Section 4.1, we consider the current state of whistleblower protections in the EU, Sweden, and the US. In Section 4.2, we outline some existing whistleblower reward programs in the US and internationally, and in Section 4.3, we conclude.

4.1 Whistleblower protections

This section provides a brief review of whistleblower protection legislation in Europe and Sweden (Section 4.1.1) and discusses means of silencing whistleblowers through non-disclosure agreements (Section 4.1.2). Finally, we consider whistleblower protections in the US and discuss their adequacy in detecting and deterring wrongdoing (Section 4.1.3).

4.1.1 EUROPE AND SWEDEN

Historically, retaliation protection for whistleblowers has been inadequate in Europe and uneven among EU member states, with some offering little to no protection. In 2013, Transparency International rated only four European countries as

having an "advanced" level of whistleblower protection. In a report by Wolfe et al. (2014) several European countries, including Germany, France, and Italy, were judged to have inadequate laws with respect to whistleblower protection.

However, the situation has changed in recent years. France enacted Sapin II in 2017, which prohibits retaliation against whistleblowers; since November 2017, whistleblower protection in Italy, which was previously limited to the public sector, has been extended to the private sector. At the EU level, on April 23, 2018, the European Commission proposed a directive providing horizontal protection for whistleblowers reporting infringements of European law. The directive includes the mandatory establishment of confidential internal reporting channels for all firms with more than 50 employees and an extensive range of public administrations, allowing for anonymous reporting (Article 5). It prohibits a wide range of retaliatory actions (Article 14), places the burden of proof on the employer in cases of alleged retaliation (Article 15), and defines "whistleblower" broadly to encompass sub-contractors, trainees, and any other person associated with a wrongdoing firm in a "work-related context" (Article 2).

Sweden recently enacted protections for whistleblowers that are retaliated against (2016: 749) through a law that came into effect on January 1, 2017. Currently, there is little to no judicial praxis surrounding the Swedish law, as the employment court where these allegations are arbitrated has not tried a single case as of June 1, 2020, though two cases have been settled according to SVT 2020. The law offers protections to those who report "serious wrongdoing," which involves any offense that can be punished with jail or comparable punishment. Employees are protected if they either report the wrongdoing to their employer (internal report) or their employer organization ("arbetsgivarorganisation"). Employees are also protected if they make an external report (e.g., publicize the information) or report it to the administrative authority, as long as two conditions apply:

> 7 § External reports
> An employee who publicizes a report externally, sends information for publication, or submits it to a government agency has a right to protection according to 4 § if:
> 1) the employee
> a) had reported the issue internally to the employer without adequate action in response to the report and without being told what actions had been taken with respect to the report, or
> b) for some other reason was justified in making the report externally, and
> 2) the employee had good grounds for the accusation of serious wrongdoing that the report concerned.[14]

14. The text in Swedish: "7§ En arbetstagare som slår larm genom att offentliggöra uppgifter eller lämna uppgifter för offentliggörande, eller genom att vända sig till en myndighet, har skydd enligt 4 § om
 1. arbetstagaren
  a) först slagit larm internt enligt 5 § utan att arbetsgivaren vidtagit skäliga åtgärder med anledning av larmet och i skälig utsträckning informerat arbetstagaren om i vilken omfattning åtgärder vidtagits, eller
  b) av något annat skäl hade befogad anledning att slå larm externt, och
 2. arbetstagaren hade fog för det påstående om allvarliga missförhållanden som larmet avser."

Notably, this law does not distinguish between reporting information to the relevant supervisor or regulatory authority and "releasing information publicly," which is more akin to leaking documents or providing them to journalists. Whereas it is reasonable to have a much lower bar for whistleblowing of the former sort to be protected, in many circumstances, the latter form of publicizing information can cause unjustified reputational damages, which warrants a higher bar for protections to be granted.

By contrast, Section 806 of the Sarbanes-Oxley Act (SOX) in the US (discussed later) provides protection against retaliation when the information is provided to "a Federal regulatory or law enforcement agency; any Member of Congress or any committee of Congress; or a person with supervisory authority over the employee (or such other person working for the employer who has the authority to investigate, discover, or terminate misconduct)." Leaks to the media are not protected under SOX.

However, the Swedish law will likely be replaced. The government recently investigated how to transpose the new EU Whistleblower Directive (SOU 2020), which suggested replacing its current regulations (2016:749).

The law (2017:630) on actions against money laundering and the financing of terrorism provides specific protections for whistleblowers in the AML context. For example, Paragraph 15 of that law states that "An operator may not subject an employee, a contractor or anyone else who on a similar basis participates in the activity to retaliation because he or she has informed about suspected money laundering or terrorist financing, internally or to the Police Authority."[15]

15. The text in Swedish: "15§ En verksamhetsutövare får inte utsätta en anställd, en uppdragstagare eller någon annan som på liknande grund deltar i verksamheten för repressalier på grund av att denne har informerat om misstänkt penningtvätt eller finansiering av terrorism, internt eller till Polismyndigheten."

4.1.2 NON-DISCLOSURE AGREEMENTS

Some employers have found ways to deter external reporting of illegal conduct to supervisory agencies by making employees sign non-disclosure agreements (NDAs) even when they are otherwise granted protections. In the Danske Bank case, the whistleblower Howard Wilkinson was asked to sign an NDA that prohibited him from speaking to anyone about what he knew "unless required by law." He was also required not to disclose the content of the non-disclosure agreement. We do not know how excessive non-disclosure agreements are in Sweden or Europe, but we do know that this was one of the main concerns of a bank employer representative when their opinion about the Swedish whistleblower law was solicited:

> The bank institutes' employer organization and the Confederation of Swedish Enterprise questions whether it should be possible to be regarded as retaliation when an employer, for example, aims a damage claim against an employee because, by blowing the whistle, they violated,

> for example, a non-disclosure clause in the employment contract.[16]

In response to the EU directive, the Confederation of Swedish Enterprise (2017: 2) argued:

> Freedom of contract is a fundamental and important legal principle that must be upheld. Deviations from the contractual freedom principle should be made with caution and only when motivated by powerful opposing interests.
>
> Trade secrets, professional secrecy, and confidentiality, etc., must be protected.

NDAs have been widely used to silence people beyond their intended purposes, such as protecting trade secrets (see, e.g., Kohn 2020, Moberly et al. 2014). Historically, the use of NDAs has increased during periods when whistleblowers gained more protections, perhaps even as a response to increased protections (see, e.g., Dworkin and Callahan 1998). Therefore, it could be useful to review these practices and evaluate how extensively non-disclosure agreements and clauses are used within banking in Sweden and the EU, examining whether they contain excessive language intended to deter employees from providing information to regulators. In Sweden's investigation into how to transpose the new EU directive, this problem is recognized as follows:

> The investigation recommends that a reporting person should not, other than in certain excepted cases, be held responsible for violating non-disclosure agreements, as for example a violation of a non-disclosure clause in a contract or non-disclosure obligations that are allowed for by the Public Access and Secrecy Act [offentlighets- och sekretesslagen].[17]

However, merely stating that employees will, on most occasions, not be held responsible for violating an NDA may not be sufficiently proactive. Kohn (2020: 18) points out that:

> Simply prohibiting improper NDAs will not prevent companies from widely utilizing NDAs to intimidate whistleblowers. Even if not enforceable in court, NDAs have a chilling effect on the vast majority of employees who sign such agreements, and do not want to risk the possibility of a counterclaim filed by their employer. Without strict sanctions against using these types of agreements, under a cost-benefit analysis, it is to a company's advantage to widely use illegal NDAs, as they will stop or intimidate a large amount of whistleblowing.

16. The text in Swedish: "Bankinstitutens Arbetsgivareorganisation och Svenskt Näringsliv ifrågasätter att det ska kunna anses som en repressalie när en arbetsgivare riktar exempelvis skadeståndsanspråk mot en arbetstagare på grund av att arbetstagaren genom larmet brutit mot t.ex. en sekretessbestämmelse i anställningsavtalet." (Regeringen 2016: 49).

17. The text in Swedish: "Utredningen föreslår att en rapporterande person inte, annat än i undantagsfall, ska kunna göras ansvarig för en överträdelse av tystnadsplikt, t.ex. en överträdelse av en sekretessklausul i ett avtal eller en tystnadsplikt som följer av offentlighets- och sekretesslagen" (SOU 2020: 27).

If this concern is not proactively dealt with in the initial transposition of the directive by prohibiting restrictive NDAs and imposing sanctions on illegal NDAs, the response by firms may be to abuse NDAs to undermine the intended effects of the directive. In the US, the SEC has been aggressively going after prohibitive NDAs. SEC Rule 21F-17(a) states that: "No person may take any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement … with respect to such communications" (Moberly et al. 2014: 91). Further, Sean Kessy, former chief of the SEC Whistleblower Office, has stated:

> We are actively looking for examples of confidentiality agreements, separat[ion] agreements, employee agreements that … in substance say "as a prerequisite to get this benefit you agree you're not going to come to the commission or you're not going to report anything to a regulator." […] if we find that kind of language, not only are we going to go to the companies, we are going to go after the lawyers who drafted it. (Moberly et al. 2014: 91)

Some of these non-disclosure clauses may not prohibit speaking to authorities outright. Instead, employers have creative ways of writing clauses that in different ways discourage external reporting. In one case, the SEC issued a penalty to a firm for the following violation: "By requiring its employees and former employees to sign confidentiality agreements imposing pre-notification requirements before contacting the SEC, KBR potentially discouraged employees from reporting securities violations to us" (SEC 2015). Pre-notification would identify the whistleblower internally.

We believe that Sweden and other EU countries should ensure that such clauses are not worded to discourage reporting to supervisory agencies, and responsible regulatory bodies must institute proper sanctions against the use of excessively prohibitive non-disclosure agreements. Adopting such policies would not give whistleblowers free rein to hand over information to journalists or publicize it freely in violation of an NDA (a significant concern for firms and banks) but legally protect the right to hand over information on wrongdoing or suspected wrongdoing to the relevant supervisory agency. Current best practices on NDAs with respect to whistleblowing are outlined in Kohn (2020: 18–19).

4.1.3 THE US EXPERIENCE AND THE INSUFFICIENCY OF PROTECTION

The US has a long experience with whistleblower protection. For example, the Whistleblower Protection Act of 1989

protects federal whistleblowers who report on government waste, corruption, and illegality from retaliation involving their employment. Even earlier, the Lloyd-La Follette Act of 1912 provided federal employees the right to communicate with members of Congress.

However, relevant actors in the United States later recognized that in addition to the need for protection, which is always inherently partial, financial rewards were necessary to compensate for the additional indirect damage that whistleblowers typically suffered and from which they could not be protected. The US has several whistleblower laws related to fraud, dating back to the False Claims Act of 1863. The IRS made some whistleblower rewards mandatory in 2006, and several US states have introduced reward schemes for exposing fraud against the government.

Frequently, legislation is introduced in response to scandals. One of the more well-known US whistleblower protection laws is the Sarbanes-Oxley Act, enacted in 2002 after the scandals at Enron and WorldCom, which protects whistleblowers who report infringements by publicly traded companies. Indeed, these scandals came to light because of whistleblowers Sherron Watkins and Cynthia Cooper, who were named persons of the year by *Time* magazine. SOX prohibited retaliation and included criminal penalties for retaliating against whistleblowers who report securities fraud. Whistleblowers who were retaliated against were offered reinstatement or back pay with interest.

However, whistleblower protections under SOX have had unclear results. Earle and Madek (2007) review SOX case law and argue that even when whistleblowers won, they were often substantially less well off after the ordeal. Consequently, the authors call whistleblower protections under SOX a "mirage." Claims of retaliation prohibited under SOX are received and managed by the Organizational Safety and Health Administration (OSHA). Of the claims closed by OSHA in fiscal year 2016, 50% were dismissed, 21% were withdrawn, and the remaining 29% were decided as "positive outcome for complainant"—a category that almost exclusively involves settlements, as only 63 cases out of 3,405 were determined to "have merit" (US Department of Labor 2017). Moberly (2007) discusses why so many whistleblowers fail under SOX. One explanation is that it is hard to prove that the whistleblowing caused retaliatory actions—employers say that they would have fired the whistleblower regardless, for example, and courts have not considered mere proximity in time between blowing the whistle and being fired as sufficient to judge the whistleblowing as the cause of the adverse employment action (see also Modesitt 2013).

In practice, evidence in this regard has been challenging to assess, as employers often try to find any alternative reason

to fire a whistleblower—disgruntled employee, poor performance, socially unsuitable—and sometimes dig up any information to support such a claim. Moreover, similar issues are likely to emerge in several EU member states, as Paragraph 93 in the Recital of the Whistleblower Directive states: "the burden of proof should shift to the person who took the detrimental action, who should then be required to demonstrate that the action taken was not linked in any way to the reporting or the public disclosure." This shifting of the burden of proof, intended to favor whistleblowers, has had unclear and ambivalent results in the US.

Moreover, SOX could not prevent the excessive risk-taking that led to the financial crisis of 2008, and the US government subsequently pushed for more powerful financial tools, including a whistleblower reward program under the Dodd-Frank Act of 2010. Protections are also problematic for other reasons. Under many protection laws, whistleblowers who are retaliated against later receive back pay and reinstatement, but only after a prolonged period of distress and legal battles. Moreover, who would want to return to an employer that just waged a legal battle against them? Financial rewards, therefore, should be thought of as compensation for the significant retaliation damages that whistleblowers often incur but courts cannot prove. Whistleblowers can be given impossible tasks, poor performance reviews, fired a year or two after reinstatement with reference to poor performance, and not given any recommendations by their employer.

Whistleblower protection laws internationally have also had unclear effectiveness. In the UK, for example, their whistleblower protection law, the Public Interest Disclosure Act of 1998, has had similar problems to those described earlier (see, e.g., All Party Parliamentary Committee 2020, Lewis 2008, TRF and BFS 2016). A recent review of whistleblower laws in 37 countries also concluded that: "Eighty-nine per cent of countries had fewer than 15 publicly reported whistleblower retaliation cases (33 out of the 37 countries in this study). Fifty-nine per cent had no reported whistleblower decisions at all (22 out of 37)" (Government Accountability Project 2021).[18] Of course, this outcome could result from a lack of retaliation against whistleblowers in these countries. Another interpretation, more consistent with the evidence on the prevalence of retaliation and corporate wrongdoing, is that employees continue to choose not to report wrongdoing even when granted protections. Moreover, even in the few cases where whistleblowers file retaliation complaints, they only succeed in 21 percent of cases (80 merit wins out of 378 merit decisions; Government Accountability Project 2021: 10).

Therefore, it is uncertain whether whistleblower protections, even with a new and improved regime under the new EU directive, will be sufficient to detect and deter corporate

18. Of course, this might be due to the absence of infringements or the deterrent effects of protection laws.

wrongdoing to a desirable degree. However, another method—providing whistleblowers with monetary rewards—looks more promising for achieving this objective.

4.2 Whistleblower reward programs

In this section, we briefly outline three different US reward programs: the False Claims Act (Section 4.2.1), the IRS Whistleblower Program (Section 4.2.2), and the SEC Whistleblower Program (Section 4.2.3), and discuss practitioners' evaluations and assessments of them (we consider independent studies in Section 5). We then outline the new US whistleblower program against AML (Section 4.2.4). Lastly, we discuss international reward programs (Section 4.2.5).

4.2.1 (US) FALSE CLAIMS ACT

The US False Claims Act is the most well-known whistleblower reward program and was initially signed into law in 1863 under President Abraham Lincoln to curb fraud in military procurement for the Union Army during the US Civil War. The program has undergone significant changes throughout the years, including an amendment in 1943 to reduce the maximum reward from no more than 50% to no more than 25% of recovered money if the whistleblower litigated the case without the DoJ, or 10% if the government litigated the case (Doyle 2009: 7). Between 1943 and 1986, these changes, together with restrictions on what kind of information makes whistleblowers eligible for rewards, led to the whistleblower or "qui tam" provisions falling almost entirely out of use (Phelps 2000: 255).

The most significant amendments came in 1986 and seem to have been pivotal in reviving the program by increasing the claims received. These amendments included retaliation protection for whistleblowers and increasing the maximum award to 30% (Doyle 2009: 8). The amendments also extended statutes of limitations, lowered the government's burden of proof, and allowed whistleblowers to bring suits with information known to the government but not released publicly (Metzger and Goldbaum 1993: 685–686). Since the 1986 amendments, False Claims Act actions have returned over $62 billion to the US Treasury, over $44 billion of which came through qui tam actions filed by whistleblowers (Cox 2020). Carson et al. (2008) estimate the ratio of costs to benefits to be between 14–1 and 52–1 for recoveries under the False Claims Act.

The act also contains safeguards against fabricated claims and wrongdoers who apply for rewards. It states that when the whistleblower initiated or planned the wrongdoing, courts can reduce the reward below 15% as they see fit (False Claims

Act, 31 U.S.C. §3730 (d)(3)). Should the whistleblower lie to the court, they risk felony charges punishable by up to five years in jail for perjury and the possibility of being convicted of other crimes related to lying under oath. Further, the False Claims Act has a reverse fee-shift for obviously frivolous claims (Engstrom 2018: 344).

An associate attorney general said of the False Claims Act in 2014 that "[Whistleblower reward laws are] the most powerful tool the American people have to protect the government from fraud." (Delery 2014), and more recently affirmed in 2020 by the assistant attorney general writing that "Whistleblowers continue to play a critical role in identifying new and evolving fraud schemes that might otherwise remain undetected" (DoJ 2020).

State-level false claim acts, which protect against false claims against the state, such as procurement fraud, also allow for whistleblower rewards in 27 US states. Many of these also reward those who blow the whistle on tax evasion (see Ventry 2014 for an overview).

4.2.2 (US) IRS WHISTLEBLOWER PROGRAM

The IRS Whistleblower Office was established following the enactment of the Tax Relief and Health Care Act of 2006. Before that, the IRS could provide rewards "for detecting and bringing to trial and punishment persons guilty of violating the internal revenue laws or conniving at the same" (IRS 2018a), but whether to provide any reward was at the agency's discretion.

Under the IRS program, a person may be convicted of a criminal offense related to tax avoidance and still receive a reward. However, a person is ineligible for a reward under the IRS program if he or she "planned and initiated" the wrongdoing. According to 7623(b), for the information provided by the whistleblower to qualify, it must "(1) relate to a tax noncompliance matter in which the tax, penalties, interest, additions to tax, and additional amounts in dispute exceed $2,000,000; and (2) relate to a taxpayer, and for individual taxpayers only, one whose gross income exceeds $200,000 for at least one of the tax years in question" (IRS 2014: 3).

The IRS writes that it will "protect the identity of the whistleblower to the fullest extent permitted by the law" (IRS 2018b). When the identity of the whistleblower is necessary to pursue investigation or examination, the IRS will inform the person before deciding whether to proceed.

4.2.3 (US) SEC WHISTLEBLOWER PROGRAM

The Dodd-Frank Act was enacted in 2010 in response to the financial crisis of 2008. In 2016, the Ontario Securities Commission implemented a bounty program modeled after the SEC program, although with fundamental differences. The

SEC's Office of Inspector General, an independent office within SEC that has the task of overseeing its programs to detect fraud, waste, and promote integrity and efficiency, praised the SEC's whistleblower program in a 2013 evaluation (Westbrook 2018: 1159). Many prominent figures in enforcement have similarly praised this program.

One former chair of the SEC, Mary Jo White, has said of the program that "it has rapidly become a tremendously effective force-multiplier, generating high-quality tips and, in some cases, virtual blueprints laying out an entire enterprise, directing us to the heart of an alleged fraud" (White 2013). White notes that:

> As the program has grown, not only have we received more tips, but we also continue to receive higher quality tips that are of tremendous help to the Commission in stopping ongoing and imminent fraud, and lead to significant enforcement actions on a much faster timetable than we would be able to achieve without the information and assistance from the whistleblower. (White 2015)

Jane Norberg, former chief at the SEC's Office of the Whistleblower, has written that "the total award amount demonstrates the invaluable information and assistance whistleblowers have provided to the agency and underscores the program's extraordinary impact on the agency's enforcement initiatives." (SEC 2016: 3).

Dodd-Frank was controversial and opposed by Republicans, who were particularly critical of the whistleblower provision—it passed narrowly, with three SEC commissioners voting in favor and two against. However, the program has been such a success that the Trump-appointed SEC commissioners all spoke favorably of the program in public comments from September 2020. For example, Chairman Jay Clayton stated that the program "has been a critical component of the Commission's efforts to detect wrongdoing and protect investors in the marketplace." The commissioners had similar positive assessments and had the following to say of the program: Hester M. Peirce: "[the whistleblower program has] become an integral part of our enforcement program"; Elad L. Roisman: "to call this program a success is an understatement"; Allison Herren Lee: "the Commission's whistleblower program has enabled us to identify and pursue fraudulent conduct, ongoing regulatory violations, and other wrongdoing that would otherwise have gone undetected"; Caroline A. Crenshaw: "whistleblowers are of tremendous value to the agency. They are a critical part of our enforcement program" (Kohn and Wilmoth 2020).

4.2.4 (US) REWARDS UNDER THE ANTI-MONEY LAUNDERING ACT OF 2020

At the end of 2020, the US introduced whistleblower rewards for persons reporting violations of Titles II and III of the Bank Secrecy Act. This decision will, in practice, mean that banks that do not adequately know their customers or facilitate transactions for suspicious persons and entities without regard to the risk they pose will run the risk that an employee with knowledge of the bank's shortcomings will turn to the US Treasury and receive a monetary reward for their information. Rewards are available for "covered judicial or administrative actions," meaning any judicial or administrative action that results in monetary sanctions exceeding $1 million. The whistleblower needs to provide "original information," meaning that (a) the information is derived from the independent knowledge or analysis of a whistleblower; (b) the information is not known to the Department of Justice, Treasury, or appropriate regulator, unless the whistleblower is the original source of this information; and (c) is not exclusively derived from an allegation made in a judicial or administrative hearing, in a governmental report, hearing, audit, or investigation, from the news media, unless the whistleblower is the source of this information.

The term "whistleblower" is defined as any individual, or two or more individuals acting jointly, providing information relating to a violation of the laws under subchapters II and III of the Bank Secrecy Act to the Treasury, in a manner established, by rule or regulation, by the Treasury. These subchapters include, among others, the reporting and record-keeping rules that are also common to the EU directives, such as being required to file a report whenever a currency transaction exceeding $10,000 is made.

When deciding the size of the reward, the Treasury should consider the following:

1. The significance of the information provided by the whistleblower to the success of the covered judicial or administrative action.
2. The degree of assistance provided by the whistleblower and any legal representative of the whistleblower in a covered judicial or administrative action.
3. The programmatic interest of the Treasury in deterring violations of the laws under subchapters II and III of this title [Bank Secrecy Act] by making awards to whistleblowers who provide information that leads to the successful enforcement of such laws.
4. Such additional relevant factors as the Treasury may establish by rule or regulation.

Rewards shall be denied if the whistleblower is or was, at the time they acquired the original information submitted to the

Treasury, a member, officer, or employee of an appropriate regulatory agency, the DoJ or the Treasury, a self-regulatory organization, or a law enforcement organization. Further, rewards shall be denied to any whistleblower convicted of a criminal violation related to the judicial or administrative action for which they could otherwise receive an award or to any whistleblower who fails to submit information to the Treasury in such form the Treasury may, by rule, require.

A fundamental difference between this program and the SEC program is that whereas the latter pays whistleblowers directly from the sanctions obtained from wrongdoers, the AML program requires Congress to make annual appropriations to pay whistleblowers. However, whistleblower compensation was not included in the bill (Kostyack 2021).

It also differs in other crucial respects. The upper limit of a reward is 30% of the sanctions obtained by the US government, but there is no lower limit as in the other US programs, and there is no obligation to pay whistleblowers a substantial amount, even if they are crucial to the success of the enforcement action. The choice not to mandate rewards may reduce the effectiveness of the program. Some suggest that since AML non-compliance usually implies other crimes such as securities fraud, tax evasion, or foreign corruption, over which the SEC and IRS have jurisdiction, whistleblowers should utilize these programs instead for protection and possibly a reward (Kostyack 2021). Like the other programs, the monetary sanctions must exceed $1 million for a reward to be considered.

The new law also differs from Dodd-Frank programs in that the anti-retaliation protections extend to those who report internally to the employer. Under Dodd-Frank, to qualify for retaliation protection, the whistleblower must report to the SEC directly. Another anomaly with this act is that compliance officers and auditors appear to be eligible for rewards, whereas these occupational roles face eligibility restrictions under Dodd-Frank.

4.2.5 INTERNATIONAL REWARD PROGRAMS

In addition to the US, many countries offer different kinds of rewards for information. Some governments also pay whistleblowers on an ad hoc basis when they are approached with information (German and UK officials have done so in relation to tax evasion, for example). Other reward programs include the Ontario Securities Commission's program, which offers rewards of 5–15% to whistleblowers who report securities violations, and Brazil's recent bill that would allow whistleblowers to obtain 5% of the public funds recovered when reporting corruption (Best 2020).

Another area where rewards have been adopted is in antitrust. Antitrust programs aim to increase the detection of practices like price-fixing but typically offer much smaller re-

wards compared to the US programs, which is the likely reason they are considered ineffective. The South Korean antitrust reward program was adopted in 2002 and caps rewards at $2.8 million, the UK program in 2008 with a reward cap at £100,000, the Hungarian program in 2010 with a reward cap at approximately €160,000, and the Slovak and Pakistani programs in 2014 (reward caps at €100,000 and €10,000, respectively).

There are also lesser-known reward provisions. Previously under the Bank Secrecy Act, whistleblowers were eligible for a discretionary reward capped at $150,000. We do not know of any whistleblower who has received a reward under this provision, nor is it widely discussed. Not all reward programs are created equal, and the correct design is crucial to generate enforcement benefits. We consider design issues in Section 5.4.

4.3 Conclusions

In the last decade, the importance of protecting whistleblowers has finally been recognized in Europe, and new legislation has been passed in several countries to protect whistleblowers against employer retaliation. At the European level, a directive has been adopted to ensure a uniform minimum level of protection for whistleblowers across member states who report violations of EU law.

More ambitious attempts to incentivize whistleblowers, compensating them with rewards for damages at least partly from the many forms of retaliation from which legal protection is impossible, have been adopted mainly in the US. Several other regulatory areas have been suggested as suitable for reward regimes: one is in the money laundering context, and, as we have seen, the US is introducing a new whistleblower reward scheme for this purpose. We next review what independent academic research has found on the effectiveness of these reward programs and relay some of the objections raised against their adoption.

5. Evidence on Whistleblower Reward Programs

THIS SECTION CONSIDERS the available evidence on the effectiveness of incentivizing whistleblowers to increase detection and deter various kinds of corporate wrongdoing. We first review whether incentivizing whistleblowers increases the detection of wrongdoing, primarily by considering data from administrations and qualitative evidence (Section 5.1). We then draw upon academic studies that explore whether protecting and incentivizing whistleblowers is an effective way of deterring further wrongdoing (Section 5.2) and conduct a brief back-of-the-envelope cost-benefit analysis of reward programs (Section 5.3). Subsequently, we weigh some different design dimensions (Section 5.4), review the often-raised objections against these programs (Section 5.5), discuss how they could be implemented in Europe (Section 5.6), and finally, we conclude (Section 5.7).

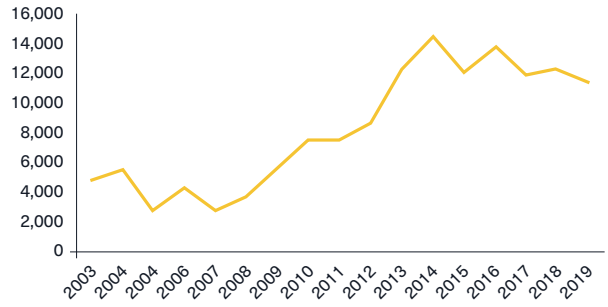
5.1 Detection: The increased quality and quantity of claims

How do whistleblower reward programs affect the number of claims received by enforcement agencies? The pattern is consistent: they increase the number of claims received in subsequent years. Figures 1 and 2 show data from SEC and IRS annual reports, and Figure 3 shows the statistics on the FCA. The reformed whistleblower program was enacted in the Tax Relief and Health Care Act of 2006.

The SEC has also seen a rising increase in claims received since the introduction of Dodd-Frank in 2011.

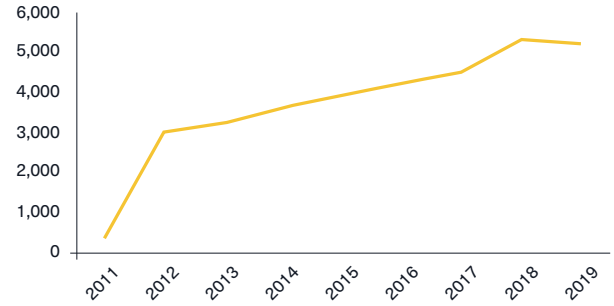
Similarly, after the 1986 amendments to the False Claims Act, the quantity of claims has increased from almost none before 1986 to over 500 claims annually since 2011. These amendments also included an increased statute of limita-

Figure 1. IRS Claims Received.



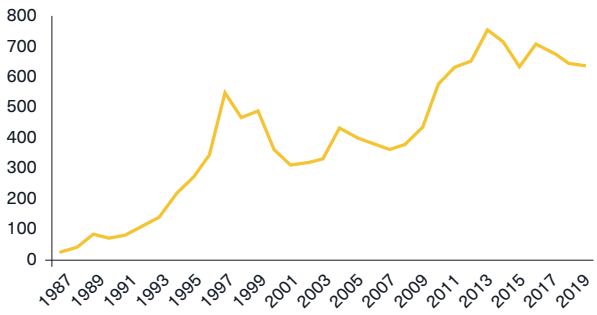
Source: IRS (2019).

Figure 2. SEC Claims Received.



Source: SEC (2019).

Figure 3. FCA Claims Received.



Source: DoJ (2019).

tions and retaliation protection, as well as other adjustments. Therefore, the increase in claims is not necessarily attributable to the provision of financial incentives.

An increased number of claims received by administrative agencies is not by itself an indicator of success unless those claims lead to enforcement actions or provide further evidence assisting in ongoing enforcement actions. It could be that many fraudsters and persons with poor information choose to submit claims for the chance of a reward and that the administrative cost of reviewing those claims outweighs the enforcement benefits gained from high-quality claims. While testimonies by officials do not support such a view, they should not be considered entirely independent or impartial assessors of these programs. In the following sections, we consider whether costs outweigh the benefits.

5.2 Deterrence

Perhaps the most desirable policy objective concerning incentivizing whistleblowers is for those incentives to have a general deterrence (preventive) effect on those who may be inclined to commit crimes. The fundamental assumption here is that by increasing the detection of crime through whistleblower incentives, the expected cost of engaging in the crime increases, leading fewer persons or organizations to be inclined to commit crimes in the first place.

The deterrence effects of various kinds of sanctions have been surprisingly hard to document, as well as the general deterrence effects of more severe criminal sanctions (see, e.g., Chalfin and McCrary 2017). Deterrence is an ideal policy outcome, as preventing crime is far less costly than dealing with it post hoc in terms of enforcement, imprisonment, and court costs. In the whistleblower reward case, the "holy grail" of evidence of increased deterrence has been obtained by several studies (see also Nyreröd and Spagnolo 2021a).

One of the most impressive and rigorous studies on the topic is by Leder-Luis (2020), who empirically measures the costs and benefits of private enforcement under the FCA. He models the decision of the whistleblower to litigate based upon socially optimal behavior and discusses the key magnitudes needed to understand efficiency. The empirical analysis pairs a novel dataset on whistleblower filings and their allegations with large samples of Medicare claims data from the period 1999–2016, which allows Leder-Luis to measure the benefits of whistleblowing, the specific deterrence effects of select whistleblower cases, the public costs of whistleblowing, and its effects on patient health outcomes.

To measure deterrence effects, Leder-Luis conducts several case studies of large settled whistleblower lawsuits and

analyzes their effects on Medicare claims and spending. To estimate counterfactuals in the absence of whistleblowing, he applies a synthetic control methodology to the case studies and then compares spending on types of medical care subjected to whistleblowing with the synthetic control group constructed of similar types of care not subject to whistleblowing.

The results suggest that the specific deterrence value of whistleblower cases is high, with specific deterrence exceeding $18 billion in the first five years for the four case studies and, on average, 6.7 times the case's settlement value. Further, he only considers specific deterrence effects and not general ones. General deterrence is when whistleblowing on a particular kind of fraudulent behavior leads to subsequent deterrence of other unrelated kinds of fraud due to a fear of being caught. This finding, therefore, constitutes a lower bound of the total deterrence effects of the cases he considers.

However, efficiency considerations also need to consider costs, such as expenditures by federal agencies overseeing and contributing to litigation and the private costs of attorneys. Leder-Luis uses federal budget data reports and estimates that total public spending totaled a mere $108.5 million in 2018. The study indicates that whistleblowing has an incredibly high return on investment, and the author argues that privatization is a promising way to proceed with antifraud enforcement.

Another recent study is Raleigh (2020), which tests the effectiveness of Dodd-Frank's whistleblower provision on reducing insider trading by corporate insiders—a violation widely regarded as more difficult to detect than corporate-level fraud. The author finds that for a sample of firms that lobbied against Dodd-Frank's whistleblower provisions, the profitability of insider purchases was significantly reduced post-Dodd-Frank relative to the profitability of other insiders. Similar results are obtained for insiders within firms with weak internal whistleblower programs, which are more likely to be sensitive to the new regulation, and for other analyses of insider transactions. The broader finding is that whistleblowers are effective deterrents of insider trading and a valuable resource for uncovering this hard-to-detect illegal activity.

Several other studies have documented deterrence effects empirically and experimentally. Amir et al. (2018) explore the effects of introducing a whistleblower hotline and reward program in the tax field, which became active in Israel in February 2013. The introduction of the policy was concurrent with a significant media campaign attracting attention to the hotline with the intention to boost knowledge and, therefore, the deterrence effects of the program. The authors find a significant increase in tax collections after the hotline was introduced in sectors with a high risk of tax avoidance. They attribute this to the deterrent effects of the hotline in conjunction with the media campaign, as the tax revenue returned through the hot-

line itself was insignificant. In 2013, around 250 events were processed by the Tax Authority of Israel, and two rewards were paid (Amir et al. 2018: 953).

Wiedman and Zhu (2018) study the deterrent effects of Dodd-Frank's whistleblower provisions by examining its impact on aggressive financial reporting among US firms. To isolate the effects of the whistleblower program, they exploit cross-sectional differences in changes that can be attributed to the whistleblower program. They measure aggressive reporting using the absolute value of abnormal accruals and find a significant reduction in abnormal accruals (approximately 11%) following the introduction of Dodd-Frank. They demonstrate that reductions in aggressive reporting are greater for firms with weaker internal reporting programs—where employees are more likely to go directly to the SEC because internal reporting is less likely to succeed.

As for experimental laboratory evidence, important for victimless crimes, Abbink and Wu (2017) conduct laboratory experiments studying collusive bribery, corruption, and the effects of whistleblower rewards on deterrence. They found that amnesty for whistleblowers and rewards strongly deter illegal transactions in a one-shot setting, but the effect is limited in repeated interactions. Bigoni et al. (2012) perform laboratory experiments on leniency policies and rewards as tools to fight collusion. They conclude that rewards financed by the fines imposed on the other cartel participants had a strong effect on average prices (returning them to a competitive level) and significant deterring and desisting effects on cartel formation. Finally, Breuer (2012) develops a controlled lab experiment and compares a tax regime without any whistleblowing mechanism with three regimes that allow subjects to blow the whistle on tax evaders. He finds that monetary rewards lead to significant increases in tax evasion reporting and that the larger the reward, the more pronounced the increase in whistleblowing.

Other studies that do not consider rewards also highlight the significance of whistleblower information. For example, Wilde (2017) studies the deterrent effects of whistleblowing on financial misreporting and tax aggressiveness. Using a dataset of retaliation complaints filed with the Occupational Safety and Health Administration between 2003 and 2010 on violations of Section 806 of the Sarbanes-Oxley Act, which prohibits retaliation against employees who provide evidence of fraud, he finds that firms subject to whistleblower allegations exhibited reduced financial misreporting and tax aggressiveness. The deterrent effect persists for at least two years after the allegations.

Johannesen and Stolper (2017) investigate the deterrent effects of whistleblowing in the offshore banking sector. They examine the stock market reaction before and after whistle-

blower Heinrich Kieber leaked important tax documents from the Liechtenstein-based LGT Bank and find abnormal stock returns in the period after the leak, noting that the market value of banks known to derive some of their revenues from offshore activities decreased. The authors interpret the leak as inducing a shock to the perceived risk of detection, thereby curbing the use of offshore bank accounts and lowering the expected future profits of banks providing access to such tax evasion technologies (Johannesen and Stolper 2017: 21–22).

Recent experimental studies, also absent rewards, show that whistleblowing is effective for reducing tax evasion. Masclet et al. (2019) conduct an experiment where taxpayers can punish tax evaders by reporting them to the authorities, even though it is costly for them to do so and they gain no material benefit. The authors find that information on other taxpayers' compliance rates, together with the opportunity to report tax evaders, has a positive and very significant effect on the level of income reported. Similarly, Bazart et al. (2020) compare a standard random-based audit scheme to a whistleblowing-based audit scheme. They find that under the whistleblowing-based scheme, as compared to the random-based scheme, the targeting of tax evaders improves, the monetary amount of tax evasion decreases, and the tax levy rises.

5.3 Are reward programs cost-effective?

Some observers have expressed concerns over the administrative costs of reward programs (Bank of England 2014, Ebersole 2011). It may be that the administrative costs outweigh the benefits received in terms of information on wrongdoing. There are few cost-benefit analyses of whistleblower reward programs and no robust ones to our knowledge.[19]

A serious evaluation of these programs would require a thorough cost-benefit analysis, including personal costs and benefits to whistleblowers, deterrence effects, costs to firms, and other costs and benefits, which is beyond our scope in this report. However, a back-of-the-envelope calculation can be done based on an estimation of only administrative costs and benefits (based on Spagnolo and Nyreröd 2021). This process may shed some light on the claim that these programs are costly to administer. The IRS and SEC programs are suitable for this purpose since the agencies provide annual reports with enough information on their administration and net benefits. The IRS has received around 117,400 claims (7623(a) and (b)) from the introduction of the program to 2017, and information submitted by whistleblowers has assisted the IRS in collecting $3.6 billion from the introduction of the program to 2017 (IRS 2017: 3). If we divide $3.6 billion by 117,400, we calculate that the average whistleblower claim

19. Attempted evaluations of this kind are often defective in several respects. Consider, for example, Filler and Markham's (2018: 335–336) attempt to put the alleged success of the SEC's whistleblower program into perspective, arguing that between 2012 and 2016, recoveries linked to whistleblowers were only about 5% of the overall recoveries from the SEC's enforcement program. However, the authors fail to compare this with the resources required to generate these enforcement benefits. The SEC whistleblower office has around 30 employees, which is a meager 0.83% of SEC employees (e.g., in 2015, the SEC had a total of 4,301 employees; SEC 2017: 14).

at the IRS generates $30,664 in returned tax money. The SEC has received around 28,100 claims since the program's introduction (SEC 2018: 20). The successful sanctions due to merited whistleblower claims amount to $1.7 billion since the program's introduction. If we divide $1.7 billion by 28,100, we find that, on average, a whistleblower claim is worth $60,498 in sanctions.

What does it cost to process each claim? We can obtain a rough idea by considering the staffing levels at the whistleblower offices and their wages. The IRS Office of the Whistleblower (OWB) has 36 full-time employees (IRS 2018c: 5). The SEC report from 2018 contains suggestive information on staffing levels at their OWB. It appears that they have more than 15 employees but fewer than 30 (SEC 2018: 6). According to PayScale.com, the average annual salary at the IRS is $74,000, and the highest is around $175,000. Taking the highest annual salary, we have 36 x $175,000 = $6,300,000. So, the annual cost of staffing at their OWB amounts to approx. $6,300,000. Now we extend this over the years 2006–2017, that is $6,300,000 x 11 = $69,300,000. We then divide this cost by the total number of claims to get the average cost per claim: $69,300,000 / 117,400 = $590 per claim. According to PayScale.com, the average annual salary at the SEC is $146,000, and the highest salary is $265,000 annually. Taking the highest annual salary, we have 30 x $265,000 = $7,950,000. $7,950,000 x 8 (2011–2018) = $63,600,000 / 28,100 = $2,263 per claim.

This back-of-the-envelope calculation does not take deterrence effects into account, nor the fact that although we have the number of claims submitted in recent years, it often takes several years until a reward is paid out. This means that while we have the total number of claims submitted to the IRS and SEC, we do not yet have the total number of rewards paid out due to these claims. Further, some of these violations may have come to the attention of enforcement agencies even without the aid of whistleblowers. Nevertheless, even if we assume that 90% of recoveries linked to whistleblower rewards would be obtained in their absence, these programs still fully pay for themselves in terms of purely administrative costs and benefits.

5.4 Important design-related aspects

Whereas many countries have adopted reward programs in recent years, these programs offer lower rewards. Similarly, the programs in antitrust offer significantly lower rewards, and the norm for these programs is to cap rewards at around $100,000. This section considers some problems with rewards in the lower ranges and argues that the US programs

are more likely to obtain desired enforcement results.

The country with the most longstanding reward program in antitrust is South Korea. What is salient about their experience is that they successively increased the reward size, starting with $19,000 in 2002, to $94,000 in November 2003 because the level of reporting did not meet expectations (KFTC 2010). The program was still not considered successful, which was partially attributed to the small reward size. The Korean Fair-Trade Commission then modified the program again in 2005, increasing the reward to approximately $1 million (Sullivan et al. 2011). Finally, the Commission increased the reward cap again in 2012 to $2.8 million (Stephan 2014). This timeline suggests that they believed more or better information could be solicited by increasing the cap of the reward program.

There is little empirical evidence to our knowledge on the success of lower-range reward programs. A cause of concern about lower, discretionary rewards is that they exist in one form or another but are rarely heard of or touted for generating substantial enforcement benefits. Some administrators of low reward programs have complained about their ineffectiveness. The chair of the UK Competition and Markets Authority, responsible for the UK's antitrust whistleblower program, has recently argued that lower rewards are inadequate:

> The £100,000 limit that it has set on such payments is far too low. It is unlikely even to cover the loss that a typical whistleblower would incur from losing his or her job. It is very unlikely to compensate either for the resulting damage to the whistleblower's career prospects, or for the distress suffered. Neither does it reflect the wider economic and social benefits that attach to successful enforcement of the law. The maximum compensation should be set at a much higher level. It should be commensurate with the financial impact, the loss of career prospects, and the distress that whistleblowers may encounter. (CMA 2019)

It is well-known that the repercussions for blowing the whistle are often substantial, as the CMA chair recognizes. While rewards in the range of $10 million may seem excessive to many, they may not be so for the livelihood of the person who reports on wrongdoing. Those with the best actionable information are often more highly placed in the organization and receive higher wages; they may also have the most to lose in the case of blowing the whistle (Engstrom 2018). Moreover, there are likely positive incentives to keep quiet that are either offered at the outset or as a response to internal whistleblowing. Call et al. (2016), for example, find that firms grant more rank-and-file employee stock options when involved in financial reporting violations, which may act as an incentive to discourage employee whistleblowing.

The issue of incentivizing those with quality information to come forward is likely compounded by a second feature of discretionary, low reward, flat-cap-programs. These programs do not proportion the willingness to report in relation to the severity of the wrongdoing, whereas under the 10–30% programs, the more egregious the wrongdoing, the higher the fine/recoveries, the higher the reward. From the point of view of the wrongdoer, the more egregious the wrongdoing, the higher the incentive to bribe internal troublemakers, and if that does not work, the threat of retaliation needs to be made more salient to dissuade potential whistleblowers. Low reward programs may therefore encourage those with poor information but a low cost of reporting to come forward while failing to persuade those with quality information but a high cost of coming forward.

Another frequently overlooked feature of the US programs is the interest they generate in the legal field. Currently, the decentralized enforcement approach has attracted many US law firms, which often work for a "contingency" fee, taking around 20–40% if the whistleblower wins. Several law firms in the US focus specifically on whistleblower representation under the SEC program and the FCA. Some have created educational and informational media for potential whistleblowers, often followed by encouragement to contact them if one is looking for representation.[20] The discretionary, low reward, flat-cap programs are unlikely to generate anything comparable in terms of an army of lawyers actively pursuing these claims, which also functions as a screening stage to assess the likelihood of the whistleblower succeeding, as lawyers are unlikely to represent whistleblowers whom they believe would not obtain a reward. This externality of the 10–30% model may be a central driver of the success of these programs, and any country or organization looking to implement a reward program—in the absence of a litigious culture like the US—should take this into account.

Other design features may also be central to the success of the US programs. Whereas a no-reward decision in the US can be appealed in tax court for the IRS program, or a whistleblower can choose to bring the claim even if the DoJ declines to join in an FCA suit, similar legal recourses are not available in many of the programs outside the US. Under these programs, the decision to reward and to what extent is entirely at the discretion of the agency, although they follow certain guidelines. Potential whistleblowers may not want to bet their financial security on the good mood of a bureaucrat without legal recourse if they feel that they have been wronged. Similarly, lawyers may be less likely to represent whistleblowers if the reward is entirely at the agency's discretion, without the possibility of appeal.

Why have policymakers gone for smaller reward sizes in-

20. A simple Google search for "whistleblower representation" generates several pages of search results listing lawyers offering their services.

ternationally and not the 10–30% regimes with documented evidence of success? One main argument for lower rewards has been that large rewards will incentivize persons to create false reports in the hope of substantial pay-outs. However, there is little to no evidence that the fabrication of evidence or false reports is a prevalent issue (see, e.g., Kohn 2014). Moreover, fabricating evidence and advancing knowingly untrue assertions can be penalized and are illegal under perjury laws. These actions may also invite defamation suits. Alternatively, penalties for frivolous claims can be written into the whistleblower law. At the same time, it may be the promise of windfall rewards that motivates individuals to take the enormous risks often associated with good faith whistleblowing.

5.5 Other concerns with reward programs

Some have raised other objections against reward programs. One is that whistleblower rewards lead to the crowding out of intrinsic moral motivation. That is, the ethical motivation to report wrongdoing is reduced when a reward is introduced because of the perceived selfishness of the act. While some studies have shown crowd out for smaller rewards and minor offenses (Feldman and Lobel 2010), there is no evidence to our knowledge that this effect has been salient with respect to the US programs. Moreover, other studies did not find moral crowd out of intrinsic motivation (Butler et al. 2019). Further, rewards are optional—a whistleblower can provide information without asking for a reward, which allows the display of intrinsic non-financial motivations. One Deutsche Bank employee who qualified for a reward did not accept it, citing moral reasons.

Another objection to reward programs is that employees will not report wrongdoing internally. Proponents suggest that employees will wait until it becomes sufficiently severe to be finable above the threshold of reward eligibility, then submit the findings to the regulator and cash a reward. There are two mitigating factors against this. First, other persons may be waiting for the wrongdoing to become sufficiently severe to report it externally, which creates substantial risks for those waiting to make an initial report. Second, most enforcement agencies consider whether the reporting was delayed, and if it was intentionally delayed, they often reduce the reward.

It has also been argued that external whistleblower reward programs more generally encourage employees to report externally rather than internally and therefore undermine internal compliance efforts. In recent decades, most firms that have been caught in corporate or banking scandals have had "codes of conduct" for their employees that usually encourage internal reporting of wrongdoing or state that the

firm prioritizes compliance. Nevertheless, if we consider the cases that we reviewed in Section 2, wrongdoing persisted for several years, suggesting a rather obvious dichotomy: either there were no internal whistleblowers, or when they had complaints, management did not do anything (or enough) about their concerns. Whistleblower reward programs directly respond to corporations' failure to comply and self-regulate, and a crucial enabler of self-regulation is to listen and take internal whistleblower complaints seriously.

However, even under these circumstances, it is still the case that most whistleblowers only approach a regulator after having raised the concern internally. For example, 83% of whistleblowers report internally before going to the SEC (Westbrook 2018: 1165). The Ethics Resource Center (2014: 29) reports that for their survey in 2013, 92% first turned to somebody inside the company to complain about misconduct. A review of qui tam filings under the False Claims Act found that 90% (113 out of 126) of those who filed qui tam had first contacted a supervisor, typically to little effect, before contacting the government (National Whistleblower Center 2011). Vandekerckhove and Phillips (2019: 217) use data on 868 whistleblower cases in the UK and conclude that "the whistleblowing process generally entails two or even three internal attempts to raise a concern before an external attempt is made, if it is made at all."

5.6 Rewards in the European AML context

Given the success of reward programs in a wide variety of regulatory areas in the US, are they suitable for the European context with respect to AML? We believe that they could be, but there are concerns about the ability of existing agencies within EU member states to manage such programs. An EBA review from 2020 has found that in several cases:

> To assess whether banks had assessed ML/TF risk in line with the requirements set out in the Directive (EU) 2015/849, competent authorities merely checked that banks had carried out a risk assessment. They did not consider themselves competent to assess whether that risk assessment was sufficiently comprehensive or made sense. (EBA 2020: 16)

The report also found that "many competent authorities had yet to set clear, regulatory expectations of banks' management of ML/TF risks. Banks in those Member States told the review team that they were not always clear about what was expected of them" (EBA 2020: 17). This conclusion suggests that at least some authorities presently do not know exactly what to

expect of banks and are not, therefore, in an authoritative and informed position to assess banks' AML/CTF risk assessments as adequate.

There are also problematic aspects in terms of the independence of European national regulators. The recent case of the German supervisor BaFin and Wirecard make it particularly evident: whistleblowers had been calling attention to the fraud for years, the *Financial Times* had made whistleblower revelations on Wirecard public, but BaFin did not intervene. Instead, they appear to have acted in defense of Wirecard and validated the firm's point of view by prohibiting short selling of its stock. Our case studies suggested that some European national supervisors have been weak enforcers of AML rules. While this does not indicate regulatory capture or revolving door issues per se, it may be a possible obstacle to enhancing supervision and enforcement that the broader economic literature has identified. Introducing several years of "cooling off," in which regulatory staff who leave the agency cannot take a position in the institutions they regulate, is a standard way of limiting this problem.

A related difference is that fines for AML non-compliance issued in Europe have historically been minimal compared to the US. In 2016, for example, BaFin issued a $44 million fine to Deutsche Bank for AML non-compliance (Reuters 2016). In comparison, Deutsche Bank has been fined $18 billion by US agencies between 2000 and the present for various offenses (data from violationtracker.org). Fines need to be substantially increased within the EU and made the go-to form of sanction to finance rewards to whistleblowers that are sufficiently large to effectively compensate them for the difficulties that follow their revelations. That said, historical fines may not be a fair comparison—as fines have been increased with the successive EU directives.

Given the suggested development toward some centralized AML supervision and enforcement, we believe it makes sense for a centralized European supervisor to manage a whistleblower reward program. Such a supervisor could more easily address concerns regarding independent and consistent enforcement, (hopefully)[21] be less susceptible to local political or industry pressure, and be adequately resourced and staffed to run a whistleblower rewards scheme. Due to the complexity of the regulatory context, such a scheme should be aimed at particularly egregious failures in AML compliance of categories (iii) and (iv), mentioned in Section 2, and with a relatively high threshold in terms of suspected laundered funds.

As outlined in Section 3.4, however, several observers are concerned and critical of the inherent ability of the current global AML regime to fulfill its promise of deterring predicate offenses or at least making life more difficult for those seeking to launder dirty money. Whistleblower reward pro-

21. The European Banking Authority, for example, has itself been in the spotlight for possible revolving door problems (European Ombudsman 2019) and a reluctance to be harder on the shortcomings of member states' supervisory agencies (Bjerregaard and Kirchmaier 2019: 38).

grams help enhance compliance with a particular regulatory regime. However, if that regime is expensive and ill-equipped to achieve its objectives, enhancing compliance is unlikely to help achieve those policy objectives. Reflecting on the observations from Section 2, one could argue that the current AML regime has not been given a fair shot given the widespread non-compliance with AML regulation in Europe.[22]

Some have raised concerns about the ability of the EU to "import" enforcement tools from a rather different legal environment such as the US. Yet, other important enforcement tools have been successfully imported and adapted to the European context. Antitrust laws introduced in Europe only a few decades ago, after a long period in which cartels were legal in many European countries, were largely inspired by the US antitrust laws enacted over half a century before. Adapting them to the very different European legal systems and cultures was uncomplicated.

Another example, even closer to whistleblower rewards, is that of leniency programs in antitrust enforcement. These programs give immunity to the first cartel member who reveals information on the cartel and continues collaborating with the antitrust authority. Leniency programs were introduced in Europe following their impressive success at increasing cartel detection in the US. After suitable legal adaptation, they have become the single most effective tool in the fight against cartels in Europe (Marvão and Spagnolo 2018). Similarly, importing these US legal innovations and adapting them to the different legal systems and cultures in Europe has not been a problem. The repetition of the argument that whistleblower rewards cannot be introduced in Europe because of differences in legal systems and cultures seems, therefore, to be mainly due to ignorance.

A final concern that has been raised is that financial rewards in themselves are unheard of or unsuitable in a European legal context. However, that is not entirely correct: Germany has sporadically paid for information on tax evaders, and the UK has paid for information on tax evaders and offers rewards for antitrust violations. Hungary, Slovenia, Lithuania, and Ukraine also pay whistleblowers who report violations.

The main hurdle to implementing rewards in a European AML context, as we see it, is the lack of an authority with the competence and independence to manage such a program. As with the Commission's responsibility for multinational antitrust cases, the current suggested response to centralize (some) form of supervision and enforcement over AML non-compliance can overcome that hurdle.

22. The disregard for correctly applying the present framework is also documented in a review by the UK's Financial Services Authority from 2011, which after conducting 35 visits to 27 banking groups in the UK concludes that with respect to high-risk customers and politically exposed persons:

> "Some banks appeared unwilling to turn away, or exit, very profitable business relationships when there appeared to be an unacceptable risk of handling the proceeds of crime. Around a third of banks, including the private banking arms of some major banking groups, appeared willing to accept very high levels of money-laundering risk if the immediate reputational and regulatory risk was acceptable."
>
> "Around a third [of banks] dismissed serious allegations about their customers without adequate review."
>
> "At more than a quarter of banks visited, RMs [relationship managers] appeared to be too close to the customer to take an objective view of the business relationship and many were primarily rewarded on the basis of profit and new business, regardless of their AML performance." (FSA 2011: 4–5)

5.7 Conclusions

In this section, we considered the evidence on the effectiveness of reward programs, objections against them, and important design-related aspects. Relevant studies suggest that whistleblower reward programs do increase the number of claims received by enforcement agencies and that these programs are cost-effective. Whistleblower reward programs effectively detect and deter securities fraud, tax evasion, and procurement fraud, which is arguably why US authorities are extending these policies to AML non-compliance. We reviewed objections to whistleblower reward programs and concluded that many of them have been vastly overstated. We also considered some important design features of the US programs as opposed to international ones: the design of a program is essential for its success; currently, most evidence favors the US 10–30% reward-size model. Lastly, we reflected on the possibilities and practicalities of introducing reward programs in Europe.

6. Conclusions and Recommendations

THE CONTINUOUS STREAM of detected AML deficiencies that enables money laundering through European banks has left many observers with the impression that the legislative efforts to curb the problem have been unsuccessful. With four transposed EU directives, and two more on the way, the problem seems as relevant today as it ever was. This environment should welcome new enforcement and supervision methods. In this report, we reviewed the case for one such method: providing whistleblowers with monetary rewards for reporting conspicuous AML non-compliance to supervisory agencies in addition to protecting them from the most evident forms of retaliation. These rewards should be sufficiently large to balance the many other, less evident forms of retaliation whistleblowers are typically subject to, against which it is impossible to offer legal protection because they are deferred or cannot be proven in court.

The US is taking this path, and we see little reason why Europe should not follow, in light of the robust evidence from independent research on the extraordinary effectiveness of these enforcement tools. There are also economic reasons for increasing enforcement within the EU of AML/CTF and sanctions rules. Typically, if a European authority fines a European bank for AML flaws, the US is unlikely to fine that bank for the same offense, according to the "non bis in idem" principle. This practice would mean that billions of dollars would be paid to EU enforcement agencies instead of to the US. However, the new AML reward program in the US is, on the face of it, likely to increase US fines against EU banks for behavior that, by and large, occurred outside of the US, as they have jurisdiction for anything involving dollar transactions. Now more European banking employees will have a clearer mandate to turn to the US Treasury and apply for rewards

with their information, and there are already several US law firms encouraging European whistleblowers to turn to them.

The US approach may also further increase the concern expressed by Danièle Nouy, the top official for prudential supervision at the ECB, who claims that it is "very embarrassing to depend on the United States to do the [AML] job. This has to change … We need a European institution that is implementing in a thorough, deep, consistent fashion this [AML] legislation in the euro area" (cited in Kirschenbaum and Véron 2018: 2).

Below, we summarize our recommendations on improving the effectiveness of the AML regime, focusing on how whistleblowers can be more effectively utilized as continuous monitors of AML non-compliance.

- In light of this report, and in particular the increasing amount of evidence from independent research discussed in Section 5, we believe that a whistleblower reward program targeting the most severe and protracted forms of AML non-compliance has the potential to be a powerful and cost-effective tool to contain predicate offenses or actual money laundering. The most promising route for implementing such a program would, we believe, be to have it run by a centralized EU-wide supervisor and enforcer, if one is created, as it requires the development of specific management skills. Such a supervisor could handle potentially severe cases involving large banks while coordinating with local supervisors and leaving them more minor cases of greater local relevance, much as is done to enforce competition law. Careful attention should be paid to how such a program is designed, advertised, and operated.
- Widespread use of prohibitive non-disclosure agreements, which has been a problem in the US, is likely to undermine the intended effects of whistleblower protections and incentives. Consultation responses by employers and bank representatives tend to stress the need for the banking business to maintain and protect such secrecy clauses. We recommend that while upholding the use of these tools for all legal business practices, European countries should also review the extent of the use of excessively prohibitive NDAs and proactively ban any that would deter whistleblowers from providing information to supervisory authorities on suspected regulatory infringements or other illegal actions.
- To reduce the risk of selective supervision and enforcement, like staff downplaying or disregarding tips about firms they worked for in the past, or from which they may expect (or hope) to obtain a job in the future, a duty to follow up on every whistleblower claim could also be imposed. Langenbucher et al. (2020) also recommend considering a duty to follow up on whistleblower claims concerning the Wirecard scandal and the German financial regulator

BaFin. It is common for supervisory agencies to employ heavily from the industry they regulate. For example, Riksrevisionen (2020: 6) notes that "[Finansinspektionen] has an extensive staff exchange with the industry. Every third manager at Finansinspektionen comes from the financial industry, and two out of three are employed there once they leave the authority." Extensive economic research that could not be discussed in this report shows that these "revolving doors" may have some benefits—like maintaining regulators' staff expertise—but may have negative costs in terms of regulatory incentives and enforcement effectiveness. There are established methods to reduce too-cozy relationships between regulator and regulated, like sufficiently long "cooling off" periods, i.e. rules prescribing that regulatory staff who leave cannot take jobs in regulated entities for several years.

› At the international level, the FATF could consider, perhaps in its membership evaluation reports, how well whistleblowers are protected and incentivized in the country or within covered institutions. The FATF could include recommendations regarding whistleblowers and highlight how effective they can be in the light of the considerable amount of independent evidence that demonstrates their positive effect on detection and deterrence. Likewise, the FATF could consider if member states impose sanctions on the use of excessively prohibitive non-disclosure agreements.

REFERENCES

ABBINK, K., AND K. WU (2017). "Reward Self-Reporting to Deter Corruption: An Experiment on Mitigating Collusive Bribery." *Journal of Economic Behavior & Organization*, 133: 256–272.

ALL PARTY PARLIAMENTARY COMMITTEE (2020). "Making Whistleblowing Work for Society." United Kingdom All Party Parliamentary Group for Whistleblowing.

AMIR, E., A. LAZAR, AND S. LEVI (2018). "The Deterrent Effect of Whistleblowing on Tax Collections." *European Accounting Review*, 75(5): 939–954.

ARTINGSTALL, D., N. DOVE, J. HOWELL, AND M. LEVI (2016). "Drivers & Impacts of Derisking." A Study by John Howell & Co. Ltd. for the Financial Conduct Authority.

BANK OF ENGLAND (2014). "Financial Incentives for Whistleblowers." Note by the Financial Conduct Authority and Prudential Regulation Authority.

BAZART, C., M. BEAUD, AND D. DUBOI (2020). "Whistleblowing vs. Random Audit: An Experimental Test of Relative Efficiency." *KYKLOS*, 73(1): 47–67.

BERGSTRÖM, M. (2018). "The Global AML Regime and the EU AML Directives: Prevention and Control." In King, C., C. Walker, and J. Gurulé (eds.) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (pp. 33–57). Palgrave Macmillan.

BEST, M. (2020). "Brazil and Papua New Guinea Consider Adding Reward Programs to Their Whistleblower Laws." Kohn, Kohn & Colapinto blog post.

BIGONI, M., C. LE COQ, S. FRIDOLFSSON, AND G. SPAGNOLO (2012). "Fines, Leniency and Rewards in Antitrust." *RAND Journal of Economics*, 43(2): 368–390.

BJERREGAARD, E., AND T. KIRCHMAIER (2019). "The Danske Bank Money Laundering Scandal: A Case Study." Copenhagen Business School.
BORLINI, L., AND F. MONTANARO (2017). "The Evolution of the EU Law Against Criminal Finance: The 'Hardening' of FATF Standards Within the EU." *Georgetown Journal of International Law*, 48(4): 1009–1062.
BRÅ (2019). "Penningtvättsbrott: En uppföljning av lagens tillämpning." Rapport 2019: 17. Brottsförebyggande rådet (BRÅ).
BREUER, L. (2012). "Tax Compliance and Whistleblowing—The Role of Incentives." University of Bonn.
BRUNSDEN, J. (2019). "EBA faces calls to reform after dropping Danske Bank probe." *Financial Times*, April.
BRUUN AND HJEJLE (2018). "Report on the Non-Resident Portfolio at Danske Bank's Estonian Branch." Danske Bank.
BUTLER, J., D. SERRA, AND G. SPAGNOLO (2019). "Motivating Whistleblowers." *Management Science*, 66(2): 605–621.
CALL, A., S. KEDIA, AND S. RAJGOPAL (2016). "Rank and File Employees and the Discovery of Misreporting: The Role of Stock Options." *Journal of Accounting and Economics*, 62: 277–300.
CARSON, T., M. VERDU, AND R. WOKUTCH (2008). "Whistle-Blowing for Profit: An Ethical Analysis of the Federal False Claims Act." *Journal of Business Ethics*, 77(3): 361–376.
CHALFIN, A., AND J. MCCRARY (2017). "Criminal Deterrence: A Review of the Literature." *Journal of Economic Literature*, 55(1): 5–48.
CLIFFORD CHANCE (2020). "Report of Investigation on Swedbank AB (publ)." Swedbank.
CMA (2019). "Letter from Andrew Tyrie to the Secretary of State for Business, Energy and Industrial Strategy." Competitions and Markets Authority.
COLAPINTO, D. (2016). "Deutsche Bank Whistleblower Should Accept SEC Whistleblower Award." Kohn, Kohn & Colapinto blog post.
COMPLIANCE WEEK (2015). "AML Compliance: 2015 Update." e-Book provided by KPMG.
CONFEDERATION OF SWEDISH ENTERPRISE (2017). "Comments on the Public Consultation on Whistleblower Protection by the Confederation of Swedish Enterprise." Public consultation response to the EU Whistleblower Directive.

COX, S. (2020). "Deputy Associate Attorney General Stephen Cox Provides Keynote Remarks at the 2020 Advanced Forum on False Claims and Qui Tam Enforcement." US Department of Justice, Office of Public Affairs.
DELERY, S. (2014). "Assistant Attorney General Stuart Delery Delivers Remarks at American Bar Association's 10th National Institute on the Civil False Claims Act and Qui Tam Enforcement." US Department of Justice, Office of Public Affairs.
DEWING, I., AND P. RUSSELL (2016). "Whistleblowing, Governance and Regulation Before the Financial Crisis: The Case of HBOS." *Journal of Business Ethics*, 134(1): 155–169.
DFS (2017). "In the Matter of Deutsche Bank AG and Deutsche Bank AG New York Branch." New York State Department of Financial Services.
DOJ (2012). "HSBC Deferred Prosecution Agreement Attachment – Statement of Facts." US Department of Justice.
DOJ (2019). "Fraud Statistics Overview." US Department of Justice.
DOJ (2020). "Justice Department Recovers Over $3 Billion from False Claims Act Cases in Fiscal Year 2019." US Department of Justice, Office of Public Affairs.
DOYLE, C. (2009). "Qui Tam: The False Claims Act and Related Federal Statutes." Congressional Research Service Report for Congress.
DUYNE, P., J. HARVEY, AND L. GELEMEROVA (2018). "A 'Risky' Risk Approach: Proportionality in the ML/TF Regulation." In King, C., C. Walker, and J. Gurulé (eds.) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (pp. 345–375). Palgrave Macmillan.
DWORKIN, T., AND E. CALLAHAN (1998). "Buying Silence." *American Business Law Journal*, 36(1): 151–191.
EARLE, B., AND G. MADEK (2007). "The Mirage of Whistleblower Protection under Sarbanes-Oxley: A Proposal for Change." *American Business Law Journal*, 44(1): 1–54.
EBA (2020). "On Competent Authorities' Approaches to the Anti-Money Laundering and Countering the Financing of Terrorism Supervision of Banks." EBA/Rep/2020/06.
EBERSOLE, D. (2011). "Blowing the Whistle on the Dodd-Frank Whistleblower Provisions." *Ohio State Entrepreneurial Business Law Journal*, 6(1): 123–174.
ENGSTROM, D. (2018). "Bounty Regimes." In Arlen, J. (ed.) *Research Handbook on Corporate Crime and Financial Misdealing* (pp. 334–362). Edward Elgar.

ESMA (2020). "Fast Track Peer Review on the Application of the Guidelines on the Enforcement of Financial Information (ESMA/2014/1293) by BaFin and FREP in the Context of Wirecard."
ETHICS RESOURCE CENTER (2014). "National Business Ethics Survey of the U.S. Workforce."
EUROPEAN COMMISSION (2020). "Communication from the Commission on an Action Plan for a Comprehensive Union Policy on Preventing Money Laundering and Terrorist Financing." 7.5.2020 C(2020) 2800 final.
EUROPEAN OMBUDSMAN (2019). "Decision in Case 2168/2019/KR. on the European Banking Authority's Decision to Approve the Request from its Executive Director to Become CEO of a Financial Lobby Group."
FAN, Z. (2017). "The 'Risk-Based' Principle of AML Management." *ACAMS Today*, September.
FATF (2017). "Anti-Money Laundering and Counter-Terrorist Financing Measures: Sweden. Mutual Evaluation Report."
FATF (2021). "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations."
FELDMAN, Y., AND O. LOBEL (2010). "The Incentives Matrix: The Comparative Effectiveness of Rewards, Liabilities, Duties, and Protections for Reporting Illegality." *Texas Law Review*, 88(6): 1151–1212.
FILLER, R., AND J. MARKHAM (2018). "Whistleblowers—A Case Study in the Regulatory Cycle for Financial Services." *Brooklyn Journal of Corporate, Financial & Commercial Law*, 12(2): 311–340.
FINANSINSPEKTIONEN (2019). "FI:s arbete mot penningtvätt och finansiering av terrorism." Rapport, 19-24575.
FINANSINSPEKTIONEN (2020a). "Varning och sanktionsavgift." FI Dnr 18-21044, FI Dnr 19-7504. Delgivning nr 1.
FINANSINSPEKTIONEN (2020b). "Swedbank Fined for Serious Deficiencies in its Measures to Combat Money Laundering." Press Release.
FINANSINSPEKTIONEN (2020c). "Anmärkning och sanktionsavgift." FI Dnr 19-8698, Delgivning nr 1.
FINANSPOLISEN (2021). "Finanspolisen informerar. Verksamheten i siffror 2020." February.
FINANSTILSYNET (2019). "Report on the Danish FSA's Supervision of Danske Bank as Regards the Estonia Case." Danish Financial Services Authority.
FINANTSINSPEKTSIOON (2019). "Response to the Report on the Danish FSA's Supervision of Danske Bank." Estonian Financial Services Authority.

FORSMAN, M. (2020). "30 Years of Combating Money Laundering in Sweden and Internationally—Does The System Function as Intended?" *Sveriges Riksbank Economic Review*, 1: 24–55.
FSA (2011). "Banks' Management of High Money-Laundering Risk Situations: How Banks Deal with High-Risk Customers (Including Politically Exposed Persons), Correspondent Banking Relationships and Wire Transfers." The United Kingdom's Financial Services Authority.
GADINIS, S. (2015). "Three Pathways to Global Standards: Private, Regulatory, and Ministry Networks." *The American Journal of International Law*, 109(1): 1–57.
GARRETT, B. (2014). *Too Big to Jail: How Prosecutors Compromise with Corporations.* Belknap Press of Harvard University Press.
GOVERNMENT ACCOUNTABILITY PROJECT (2021). "Are Whistleblowing Laws Working? A Global Study of Whistleblower Protection Litigation." Government Accountability Project and International Bar Association.
HALLIDAY, T. C., M. LEVI, AND P. REUTER (2014). "Global Surveillance of Dirty Money: Assessing Assessments of Regimes to Control Money-Laundering and Combat the Financing of Terrorism." Center on Law & Globalization. University of Illinois College of Law and American Bar Foundation.
HALLIDAY, T. C., M. LEVI, AND P. REUTER (2019). "Anti-Money Laundering: An Inquiry into a Disciplinary Transnational Legal Order." *Journal of International, Transnational, and Comparative Law*, 4: 1–25.
HOUSE OF REPRESENTATIVES (2016). "Too Big to Jail: Inside the Obama Justice Department's Decision Not to Hold Wall Street Accountable." Report Prepared by the Republican Staff of the Committee on Financial Services.
HSBC (2017). "Annual Report and Accounts 2017." HSBC Holdings plc.
IRS (2014). "IRS Whistleblower Program: Annual Report to Congress." IRS Whistleblower Office.
IRS (2017). "IRS Whistleblower Program: Annual Report to Congress." IRS Whistleblower Office.
IRS (2018a). "History of the Whistleblower Informant Program."
IRS (2018b). "Confidentiality and Disclosure for Whistleblowers."
IRS (2018c). "IRS Whistleblower Program: Annual Report to Congress." IRS Whistleblower Office.
IRS (2019). "IRS Whistleblower Program: Annual Report to Congress." IRS Whistleblower Office.

JOHANNESEN, N., AND T. STOLPER (2017). "The Deterrence Effect of Whistleblowing—An Event Study of Leaked Customer Information from Banks in Tax Havens." Working Paper of the Max Planck Institute for Tax Law and Public Finance No. 2017-4.

JOHNSON, M., AND D. MCCRUM (2020). "Wirecard Processed Payments for Mafia-Linked Casino." *Financial Times*, August.

JPP (2019). "Joint Position Paper by the Ministers of Finance of France, Germany, Italy, Latvia, the Netherlands, and Spain."

KFTC (2010). "Annual Report." Korean Fair-Trade Commission.

KIRSCHENBAUM, J., AND N. VÉRON (2018). "A Better European Architecture to Fight Money Laundering." Peterson Institute for International Economics. Policy Brief 18-25.

KIRSCHENBAUM, J., AND N. VÉRON (2020). "A European Anti-Money Laundering Supervisor: From Vision to Legislation." Peterson Institute for International Economics, January.

KKC (2020). "Bradley Birkenfeld." Kohn, Kohn & Colapinto, LLP.

KOHN, S. (2014). "The Importance of Whistleblower Rewards in Combating International Corruption." National Whistleblower Center, Washington DC.

KOHN, S. (2020). "Memorandum: Implementation of the European Union Whistleblower Protection Directive." Kohn, Kohn & Colapinto, LLP.

KOHN, S., AND M. WILMOTH (2020). "The 100 Whistleblowers Who Changed Wall Street." *The National Law Review*.

KOSTYACK, B. (2021). "New Anti-Money Laundering Whistleblower Law Becomes Effective After Congress Overrides Presidents Trump's Veto of the NDAA." Kohn, Kohn, and Colapinto blog post.

LANGENBUCHER, K., C. LEUZ, J. KRAHNEN, AND L. PELIZZON (2020). "What Are the Wider Supervisory Implications of the Wirecard Case?" Study requested by the European Parliament ECON committee.

LEDER-LUIS, J. (2020). "Whistleblowers, Private Enforcement, and Medicare Fraud." Working Paper. Massachusetts Institute of Technology.

LEVI, M. (2018). "Punishing Banks, Their Clients, and Their Clients' Clients." In King, C., C. Walker, and J. Gurulé (eds.) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (pp. 273–293). Palgrave Macmillan.

LEVI, M., P. REUTER, AND T. HALLIDAY (2018). "Can the AML System Be Evaluated Without Better Data?" *Crime, Law and Social Change*, 69(2): 307–328.
LEWIS, D. (2008). "Ten Years of Public Interest Disclosure Legislation in the UK: Are Whistleblowers Adequately Protected?" *Journal of Business Ethics*, 82(2): 497–507.
LEXISNEXIS (2017). "The True Cost of Anti-Money Laundering Compliance: European Edition."
LEXISNEXIS (2019). "True Cost of AML Compliance Study: United States & Canada Edition."
MAGNUSSON, D. (2009). "The Costs of Implementing the Anti-Money Laundering Regulations in Sweden." *Journal of Money Laundering Control*, 12(2): 101–112.
MARVÃO, C., AND G. SPAGNOLO (2018). "Cartels and Leniency: Taking Stock of What We Learnt." In Corchón, L., and M. Marini (eds.) *Handbook of Game Theory and Industrial Organization, Volume II* (pp. 57–90). Edward Elgar.
MASCLET, D., C. MONTMARQUETTE, AND N. VIENNOT-BRIOT (2019). "Can Whistleblower Programs Reduce Tax Evasion? Experimental Evidence." *Journal of Behavioral and Experimental Economics*, 83: 1–15.
MAXIMILIAN, F., AND J. TEICHMANN (2020). "Money-Laundering and Terrorism-Financing Compliance—Unsolved Issues." *Journal of Money Laundering Control*, 23(1): 90–95.
MAXWELL, N., AND D. ARTINGSTALL (2017). "The Role of Financial Information-Sharing Partnerships in the Disruption of Crime." Royal United Services Institute for Defence and Security Studies (RUSI), Occasional Paper, October.
MCCRUM, D., AND S. PALMA (2019). "Wirecard: Inside an Accounting Scandal." *Financial Times*, February.
MCCRUM, S., S. PALMA, AND O. STORBECK (2021). "Wirecard's Reluctant Whistleblower Tells His Story: 'They Tried to Destroy Me.'" *Financial Times*, May.
METZGER, R., AND R. GOLDBAUM (1993). "Retroactivity of the 1986 Amendments to the False Claims Act." *Public Contract Law Journal*, 22(4): 684–705.
MIETHE, T., AND J. ROTHSCHILD (1994). "Whistleblowing and the Control of Organizational Misconduct." *Sociological Inquiry*, 64(3): 322–347.
MOBERLY, R. (2007). "Unfulfilled Expectations: An Empirical Analysis of Why Sarbanes-Oxley Whistleblowers Rarely Win." *William & Mary Law Review*, 49(1): 65–155.
MOBERLY, R., J. A. THOMAS, AND J. ZUCKERMAN (2014). "De Facto Gag Clauses: The Legality of Employment Agreements That Undermine Dodd-Frank's Whistleblower Provisions." *Journal of Labor and Employment Law*, 30(1): 87–120.

MODESITT, N. (2013). "Why Whistleblowers Lose: An Empirical and Qualitative Analysis of State Court Cases." *University of Kansas Law Review*, 62(1): 165–194.
NAHEEM, M. (2016). "Risk of Money Laundering in the US: HSBC Case Study." *Journal of Money Laundering Control*, 19(3): 225–237.
NATIONAL WHISTLEBLOWER CENTER (2011). "Comments and Legal Guidance Concerning Proposed Rule 240.21 F-8 for Implementing Whistleblower Provisions of the Dodd-Frank Act Reply to February 15th Letter from Chamber of Commerce." March.
NYRERÖD, T., AND G. SPAGNOLO (2021a). "Myths and Numbers on Whistleblower Rewards." *Regulation and Governance*, 15(1): 82–97.
NYRERÖD, T., AND G. SPAGNOLO (2021b). "Surprised by Wirecard? Enablers of Corporate Wrongdoing in Europe." SITE Working Paper No. 54.
OCC (2017). "Lessons Learned: Review of Supervision of Sales Practices at Wells Fargo." Office of the Comptroller of the Currency.
PARLIAMENTARY COMMISSION ON BANKING STANDARDS (2013). "Changing Banking for Good." Report of the Parliamentary Commission on Banking Standards.
PHELPS, J. M. (2000). "False Claims Act's Public Disclosure Bar: Defining the Line Between Parasitic and Beneficial." *Catholic University Law Review*, 49(1): 247–278.
POL, R. (2018). "Uncomfortable Truths? ML=BS and AML=BS^2." *Journal of Financial Crime*, 25(2): 294–308.
POL, R. (2020). "Response to Money Laundering Scandal: Evidence-Informed or Perception Driven?" *Journal of Money Laundering Control*, 23(1): 103–121.
RALEIGH, J. (2020). "The Deterrent Effect of Whistleblowing on Insider Trading." University of Minnesota Working Paper.
RAMACHANDRAN, V., M. COLLIN, AND M. JUDEN (2018). "De-Risking: An Unintended Negative Consequence of AML/CFT Regulation." In King, C., C. Walker, and J. Gurulé (eds.) *The Palgrave Handbook of Criminal and Terrorism Financing Law* (pp. 237–273). Palgrave Macmillan.
REGERINGEN (2016). "Lagrådsremiss. Ett särskild skydd för arbetstagare som slår larm om allvarliga missförhållanden."
REGERINGEN (2017). "Regeringens proposition 2016/17: 173. Ytterligare åtgärder mot penningtvätt och finansiering av terrorism."
REUTER, P., AND E. M. TRUMAN (2004). *Chasing Dirty Money: The Fight Against Money Laundering*. Peterson Institute for International Economics.

REUTERS (2016). "Bafin Fines Deutsche Bank for Anti-Money Laundering Flaws: Source." June.
REUTERS (2018). "Estonia Arrests Ten in Danske Bank Money Laundering Inquiry." December.
REZNIK, I., AND O. UMMELAS (2019). "A Banker Reveals the Bonus Culture Behind a $220 Billion Scandal." *Bloomberg*, October.
RIKSREVISIONEN (2020). "Finansinspektionens arbete för att motverka intressekonflikter." RIR 2020: 18.
ROBINSON, T. (2019). "Blowing Whistle on Dirty Money 'Wrecked My Life.'" *BBC Panorama*, October.
RUSI (2019). "Financial Action Task Force Strategic Review." Panel discussion by RUSI's Centre for Financial Crime & Security Studies, November.
SCHWARTZKOPFF, F. (2018). "Danske's 402% Return Should Have Raised Red Flag, FSA Says." *Bloomberg*, May.
SEBAG, G. (2019). "HSBC Swiss Unit to Pay $329 Million in Belgian Tax Settlement." *Bloomberg*, August.
SEC (2015). "SEC: Companies Cannot Stifle Whistleblowers in Confidentiality Agreements." Press Release 2015-54.
SEC (2016). "Annual Report to Congress: Whistleblower Program." Office of the Whistleblower.
SEC (2017). "Annual Report to Congress: Whistleblower Program." Office of the Whistleblower.
SEC (2018). "Annual Report to Congress: Whistleblower Program." Office of the Whistleblower.
SEC (2019). "Annual Report to Congress: Whistleblower Program." Office of the Whistleblower.
SERGEANT, C. (2002). "Risk-Based Regulation in the Financial Services Authority." *Journal of Financial Regulation and Compliance*, 10(4): 329–335.
SILVA, P. (2019). "Recent Developments in EU Legislation on Anti-Money Laundering and Terrorist Financing." *New Journal of European Criminal Law*, 10(1): 57–67.
SNS (2019). "SNS/SHOF Finance Panel: Money Laundering and the Financial Sector—Talk with Europol's Former Head." February.
SOU (2020). *Ökad trygghet för visselblåsare*. Betänkande av Utredningen om genomförande av visselblåsardirektivet. Arbetsmarknadsdepartementet. SOU 2020:38.
SPAGNOLO, G., AND T. NYRERÖD (2021). "Financial Incentives for Whistleblowers: A Short Survey." In van Rooij, B., and D. Sokol (eds.) *The Cambridge Handbook of Compliance* (pp. 341–350). Cambridge University Press.
STEPHAN, A. (2014). "Is the Korean Innovation of Individual Informant Rewards a Viable Cartel Detection Tool?" CCP Working Paper 14-3.
SULLIVAN, K., K. BALL, AND S. KLEBOLT (2011). "The Potential Impact of Adding a Whistleblower Reward Provision to ACPERA." *The Antitrust Source*, October.

SVEDBERG HELGESSON, K., AND U. MÖRTH (2018). "Client Privilege, Compliance and the Rule of Law: Swedish Lawyers and Money Laundering Prevention." *Crime, Law and Social Change*, 69(2): 227–248.
SVT (2019). "Misstänkt penningtvätt i Swedbank." *Sveriges Television*, February.
SVT (2020). "Stämningen från Båstadsvisslare kan bli första att avgöras av domare." *Sveriges Television*, June.
SWEDISH NATIONAL RISK ASSESSMENT (2019). "National Risk Assessment of Money Laundering and Terrorist Financing in Sweden 2019." Report by sixteen Swedish authorities and the Swedish Bar Association.
TRF AND BFS (2016). "Protecting Whistleblowers in the UK: A New Blueprint." Thomas Reuter Foundation and Blueprint for Free Speech.
UNGER, B. (2011). "Money Laundering Regulation: From Al Capone to Al Qaeda." In Levi-Faur, D. (ed.) *Handbook on the Politics of Regulation* (pp. 615–628). Edward Elgar.
UNGER, B. (2017). "Offshore Activities and Money Laundering: Recent Findings and Challenges." Directorate-General for Internal Policies, European Parliament.
UNGER, B. (2020). "Improving Anti-Money Laundering Policy." Study requested by the ECON Committee, European Parliament.
UNGER, B., M. SIEGEL, J. FERWERDA, W. DE KRUIJF, M. BUSUIOIC, K. WOKKE, AND G. RAWLINGS (2006). "The Amounts and the Effects of Money Laundering." Report for the Dutch Ministry of Finance.
UNODC (2011). "Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes." Research Report, United Nations Office on Drugs and Crime.
US DEPARTMENT OF LABOR (2017). "Whistleblower Investigation Data Factsheet."
US SENATE (2012). "U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History." United States Senate, Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs.
VANDEKERCKHOVE, W., AND A. PHILLIPS (2019). "Whistleblowing as a Protracted Process: A Study of UK Whistleblower Journeys." *Journal of Business Ethics*, 159(1): 201–219.
VENTRY JR, D. J. (2014). "Not Just Whistling Dixie: The Case For Tax Whistleblowers in the States." *Villanova Law Review*, 59(3): 425–502.
WESTBROOK, A. (2018). "Cash for Your Conscience: Do Whistleblower Incentives Improve Enforcement of the Foreign Corrupt Practices Act?" *Washington and Lee Law Review*, 75(2): 1097–1167.

WHITE, M. (2013). "Remarks at the Securities Enforcement Forum." Washington D.C. Speech, October.
WHITE, M. (2015). "The SEC as the Whistleblower's Advocate." Speech at Ray Garrett, Jr. Corporate and Securities Law Institute—Northwestern University School of Law, Chicago, Illinois. April.
WIEDMAN, C., AND C. ZHU (2018). "Do the SEC Whistleblower Provisions of Dodd-Frank Deter Aggressive Financial Reporting?" 2018 Canadian Academic Accounting Association Annual Conference.
WILDE, J. (2017). "The Deterrent Effect of Employee Whistleblowing on Firms' Financial Misreporting and Tax Aggressiveness." *The Accounting Review*, 92(5): 247–280.
WILKINSON, H. (2018). "Money Laundering: What Happened in Estonia." Public Hearing on Money Laundering at Danske Bank. The Business, Growth and Export Committee. Danish Parliament (Folketinget). November.
WOLFE, S., M. WORTH, S. DREYFUS, AND A. BROWN (2014). "Whistleblower Protection Laws in G20 Countries. Priorities for Action." Blueprint for Free Speech, The University of Melbourne, Griffith University, and Transparency International Australia.
WORTH, M. (2020). "The Wirecard Scandal and the Beauty of Anonymous Whistleblowing." *Whistleblower News Network*, June.
WORTHINGTON, E., AND M. CHRISTODOULOU (2020). "Former ANZ Executive Uses New Whistleblower Laws to Sue ANZ Bank." *ABC News*, July.
YEOH, P. (2014). "Enhancing Effectiveness of Anti-Money Laundering Laws Through Whistleblowing." *Journal of Money Laundering Control*, 17(3): 327–342.

MONEY LAUNDERING is estimated to annually amount to between 2 and 5 percent of global GDP. Also, less than 1 percent of proceeds laundered via the financial system are seized and frozen by regulatory and law enforcement agencies.

The fight against money laundering has been an international priority for at least thirty years, but the problem seems to be as pertinent as ever. In the report, this is illustrated by describing a number of recent cases of anti-money laundering non-compliance in financial institutions.

Globally, the Financial Action Task Force (FATF) is the primary standard setter for combating money laundering and terrorist financing. It has managed to achieve broad compliance among its over 180 member countries. However, its "outcome effectiveness" has recently been called into question.

The authors assess one new supervisory and enforcement method: offering financial rewards to whistleblowers who bring particularly valuable information regarding severe cases of anti-money laundering non-compliance in financial institutions to supervisory law enforcement agencies. In doing this, the authors draw on the experience of whistleblowing in the United States and what academic research has shown regarding their effectiveness.

Giancarlo Spagnolo is a professor of economics at the Stockholm Institute of Transition Economics (SITE) at the Stockholm School of Economics.

Theo Nyreröd is a PhD candidate at Brunel Law School.

ISBN 978-91-88637-69-7