THE DETECTION OF FOREIGN BRIBERY

THE ROLE OF WHISTLEBLOWERS AND WHISTLEBLOWER PROTECTION

OECD

Please cite this publication as:

OECD (2017), *The Detection of Foreign Bribery, Chapter 2. The Role of Whistleblowers and Whistleblower Protection,*
www.oecd.org/corruption/the-detection-of-foreign-bribery.htm

Foreword

This document, originally published in the OECD study on The Detection of Foreign Bribery, looks at the key role that whistleblowers and whistleblower protection can play in the detection of foreign bribery when legal frameworks and appropriate channels are in place to report alleged instances to law enforcement authorities. It explores the various approaches to encourage whistleblower reporting, including by providing effective legal protection from reprisals, with a view to sharing these practices and improving countries' capacity to detect and ultimately step up efforts against transnational bribery.

This document was drafted by Leah Ambler under the coordination of France Chain, Senior Legal Analyst, from the Anti-Corruption Division of the OECD Directorate for Financial and Enterprise Affairs. The development of this document benefited from inputs from the Korean Anti-Corruption and Civil Rights Commission, the Dutch Whistleblower Authority and the OECD Public Governance Directorate.

The OECD study on The Detection of Foreign Bribery covers ten "primary" detection sources which have been, or could be expected to be, at the origin of foreign bribery investigations. It uses material collected through country reviews undertaken by the OECD Working Group on Bribery in International Business Transactions (OECD WGB) in the context of its monitoring of countries implementation of the Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (OECD Anti-Bribery Convention). Annex 1 describes the scope and methodology of the study and Annex 2 provides key findings from the study.

Introduction

Whistleblowers are an important source of foreign bribery cases and they often provide pivotal evidence for a successful prosecution. However, only 2% (5 cases) of foreign bribery schemes resulting in sanctions was detected by whistleblowers, most of who did not report directly to law enforcement authorities but instead raised the alarm internally within their organisation.[1] Detection through whistleblower reporting to law enforcement authorities is rarely discussed in public by such authorities because of the need to protect the whistleblowers involved. The Luxleaks case has put the spotlight again on the role of whistleblowers in promoting the public interest. The following case is an example of whistleblower reporting leading to a successful law enforcement outcome.

Box 1. **United States Case Study: Mikerin Case (2015)**

US-based Transport Logistics International (TLI), a company specialising in the transportation of nuclear fuel for civilian use between the Russian Federation and the United States, conspired with others, including its US-based executives, to pay approximately USD 2 million in bribes, between 2004 and 2013, to Vadim Mikerin, a foreign official with Techsnabexport (Tenex), a Russian state-owned corporation that sold and transported nuclear fuel on behalf of the Russian Federation and its nuclear agency, Rosatom. Thus far, three people have pleaded guilty to FCPA-related offences, including Vadim Mikerin who pleaded guilty to a conspiracy to commit money laundering and received a sentence of 48 months of imprisonment. The case was detected by a government informant who was asked by Mikerin to pay and launder bribes. That informant advised the FBI who opened an investigation and discovered additional bribe payments by TLI.

The reluctance of whistleblowers to report to law enforcement authorities is likely due to the lack of effective legal protections in many Parties to the OECD Anti-Bribery Convention. According to a 2016 OECD study, of the 43 Parties to the Anti-Bribery Convention, only 14 had adopted measures that satisfactorily meet the 2009 Anti-Bribery Recommendation's provisions on private sector whistleblower protection.[2] The WGB has stated that the implementation of effective whistleblower protection frameworks is a horizontal issue that confronts many Parties to the OECD Anti-Bribery Convention.

The 2009 Anti-Bribery Recommendation recommends that countries ensure that "appropriate measures are in place to protect from discriminatory or disciplinary action public and private sector employees, who report in good faith and on reasonable grounds to the competent authorities suspected acts of bribery" (OECD, 2009a, Recommendation IX iii). The OECD Recommendation on Public Integrity recommends "clear rules and procedures for reporting suspected violations of integrity standards, and […] protection in law and practice against all types of unjustified treatment as a result of reporting in good faith and on reasonable grounds." It further advises "providing alternative channels for reporting suspected violations of integrity standards, including when appropriate the

[1] This figure is based on publicly-available court decisions, documents in finalised cases of bribery of foreign public officials, and other sources (such as media reports). This figure has not been validated by the States Parties to the OECD Anti-Bribery Convention, particularly those that have strict confidentiality rules that preclude associating whistleblowers with finalised cases.

[2] OECD (2016b), pge 105. At the time of and after publication of this study, several countries enacted whistleblower protection legislation that has not yet been evaluated by the WGB.

possibility of confidentially reporting to a body with the mandate and capacity to conduct an independent investigation." (OECD, 2016e, Recommendations 9b and 9c)

There is no internationally accepted definition of "whistleblower". A whistleblower can be any person who reports suspicions of bribery of foreign public officials to law enforcement authorities, an employee who reports internally to the company, or third persons who report to law enforcement or the media. Whistleblowers who report are sometimes also involved in the offence. Protection should be afforded to whistleblowers regardless of their motives in making the disclosure and regardless of whether they report directly to law enforcement, or report internally - first within the company, or to the media, an elected government official or to civil society (for example, an advocacy group or a non-governmental organisation). The importance of whistleblower protection in facilitating detection through self-reporting, investigative journalism and reporting by the accounting and legal professions is addressed in other chapters of the report. This chapter will explore various approaches to encourage whistleblower reporting, including by providing effective legal protection from reprisals.

1. How can whistleblowers be encouraged to report foreign bribery allegations to law enforcement authorities?

1.1 Raise awareness

Raising awareness of protections afforded to whistleblowers and of the channels for reporting is essential to ensure the effectiveness of any whistleblower reporting framework. Whistleblowers must know where, how, and when to report; that their identity as a whistleblower will be kept confidential; and also that they will be protected with anti-retaliation remedies. Raising awareness of the importance of whistleblowers can promote a "speak up" culture and de-stigmatise the disclosure of wrongdoing. For example, the Office of the Whistleblower (OWB) of the **US** Securities and Exchange Commission (SEC) participates in public engagements aimed at promoting and educating the public concerning the US SEC's whistleblower programme. Target audiences include potential whistleblowers, whistleblower counsel, and corporate compliance counsel and professionals. The OWB also aims to promote and educate the public about the whistleblower programme through its website (www.sec.gov/whistleblower). The website contains detailed information about the programme, copies of the forms required to submit a tip or claim an award, a listing of enforcement actions for which a claim for award may be made, links to helpful resources, and answers to frequently asked questions.

Country practices: Raising awareness of whistleblowing frameworks	
Korea: Anti-Corruption and Civil Rights Commission (ACRC)	Since the entry into force of Korea's Public Interest Whistleblower Act, the Anti-Corruption and Civil Rights Commission (ACRC), the body responsible for its implementation, has undertaken several awareness-raising initiatives, including both in the general anti-corruption context, such as through the annual ACRC Policy Roundtable for Foreign Businesses in Korea, where the ACRC Chairperson invites leaders of foreign businesses operating in Korea to discuss Korea's anti-corruption policy; and in whistleblower protection-focused contexts, including • workshops on dealing with whistleblower reporting and protection in the public and private sectors (2012, 2014), • lectures tailored to different groups in society to raise awareness of public interest whistleblowing and protection: public organisations, businesses, and the general public (about 3,500 participants in 2011, 2012), • yearly distribution of promotional materials since 2013, including TV commercial, posters, leaflets, banners on internet portals, on-board video materials for train cabins, • update and distribution of PPT materials on whistleblower reporting and protection for training of employees of public organisations (2012, 2013, 2014, 2016), • distribution and operation of online training on public interest whistleblowing (2014, 2016), • distribution of the whistleblower protection guide for companies (2015), • and newspaper commercials (2014), e-book on public interest reporting best practices (2015), radio commercials (2016). The ACRC also made efforts to raise awareness on public interest whistleblowing among the youth by publishing webtoons and mobile messenger emoticons (2012). About 16% of the public were aware of the whistleblower protection system in 2011, and the figure jumped to 23.6% in 2012 and 28.4 in 2016. *Source: Korea Phase 3 Written Follow-Up Report (OECD, 2014)); Korea ACRC*
Ireland: Integrity at Work Initiative	Partnerships between government and civil society can also promote whistleblower reporting and protection. A recent example of such collaboration is Ireland's Integrity at Work (IAW) Initiative, which aims to assist employers to comply with the Protected Disclosures Act (2014) and foster workplaces where people feel safe to speak up about wrongdoing. The IAW along with Ireland's Transparency Legal Advice Centre (TLAC) – an independent law centre established by TI Ireland that provides free specialist legal advice on protected disclosures – are run by TI Ireland with funding from the Irish Department of Public Expenditure and Reform and Department of Justice and Equality.* Members of the IAW programme come from all sectors: public, private and not-for-profit. To date, 24 organisations have joined or signalled their intention to join IAW. Two IAW Forums (seminars and workshops) have been delivered to over 100 participants between December 2016 and June 2017, focusing on providing expert guidance to employers on important issues such as assessments and investigations, complying with the Protected Disclosures Act, and related topics. As a result, there has been an increase of over 200% in the proportion of whistleblowers calling the Speak Up helpline since it was established in 2011. TLAC has also been providing free legal advice to clients since March 2016. TLAC's clients are (or were) employed in a variety of sectors including health, social care and government. ** For more information, see: http://transparency.ie/integrity-work.*

1.2 Provide clear reporting channels

The 2009 Anti-Bribery Recommendation urges countries to ensure that easily accessible channels are in place to report suspected acts of foreign bribery to law enforcement authorities, in accordance with member countries' legal principles (OECD, 2009, Recommendation IX i). It is important to ensure that reports can be made by various means (e.g., phone, online, mail, and fax) to allow whistleblowers to choose the channel most adapted to their circumstances. For example, whistleblowers in open-space offices might be reluctant to use online or phone hotlines during work hours and may prefer to report outside of work hours by other means. Clear reporting channels should not only be put in place, but also publicised. The WGB has recommended that 17 countries raise awareness in the public and private sectors about the available channels for making reports.[3]

The US SEC's OWB was established under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 and began operating in 2011. In 2017, the OWB received over 4 400 tips, an increase of almost 50% since 2012 (its first full year of operation). Beginning in August 2011, individuals wishing to participate in the US SEC's whistleblower programme have been required to submit their tip through a "Submit a Tip" button on the SEC's online portal or in hard copy on a specific form ("Form TCR"). OWB raised awareness of the online portal by (1) publicising it actively through participation in webinars, presentations, speeches, press releases, and other public communications; (2) establishing a publicly-available whistleblower hotline and directing callers to the online portal; and (3) in meetings with whistleblowers, potential whistleblowers and their counsel and corporate compliance counsel and professionals to promote the online portal.

Country practice: Complaint or Referral Portal	
United States: "Submit a Tip", US SEC, Office of the Whistleblower's Online Tip	US Exchange Act Rule 21F-9 provides whistleblowers the option to submit tips either electronically through an online portal that feeds directly into the Tips, Complaints or Referrals (TCR) System or by mailing or faxing a hard-copy Form TCR directed to OWB. This flexibility supports whistleblowers who may not have access to a computer or who may prefer to submit their information in hard copy. In cases where whistleblowers elect to submit a hard-copy Form TCR, OWB manually enters the tip into the TCR System so that it can be appropriately reviewed, assigned, and tracked in the same manner as tips received through the online portal. OWB's website (www.sec.gov/whistleblower) contains detailed information about the programme, copies of the forms required to submit a tip or claim an award, a listing of enforcement actions for which a claim for award may be made, links to helpful resources, and answers to frequently asked questions. *Source: US SEC, OWB Annual Report, 2016*

[3] Bulgaria, Estonia, Finland, Germany, Hungary, Iceland, Ireland, Israel, Italy, Korea, Luxembourg, Mexico, New Zealand, Slovak Republic, Slovenia, South Africa and Turkey. This list refers to the countries that received such recommendation in the context of their Phase 3 evaluation by the WGB. In the case of Bulgaria, Estonia, Finland, Germany, Iceland, Italy, Mexico, Slovak Republic, recommendations were made to both ensure that appropriate measures are in place to protect whistleblowers and take steps to raise awareness of these mechanisms.

The **Dutch** Whistleblowers Authority Act (*Wet Huis voor Klokkenluiders*) entered into force on 1 July 2016. The purpose of the Act is to improve ways to report a concern about wrongdoing within organisations and to offer better protection to those who do so. The Act also provides for the establishment of a Whistleblowers Authority which is mandated to receive, investigate and refer protected disclosures or alleged retaliation or a combination of both. Pursuant to the Act, Dutch companies with 50 or more employees must establish internal reporting and protection mechanisms. The Act then provides for a tiered approach to reporting: first internally within the company, then to the relevant authority and finally to the Whistleblowers Authority as a last resort. There are exceptions to this tiered approach in cases of emergency; where the company or authority has not put in place the required reporting mechanism; or when highest level management is involved in the wrongdoing. The Whistleblowers Authority Act also gives the employee the right to obtain confidential advice about the best course of action before making a report, either from the company's confidential counsellor, a Whistleblowers Authority advisor or a private lawyer or other advisor. In its first 6 months of operation, 532 people contacted the Whistleblowers Authority's Advice Department; 70 of these requests for advice were considered as whistleblower cases; 183 were still under evaluation as of December 2016. In terms of subject-matter, 33% of requests involved an issue in the public sector; 32% involved an issue in the private sector; and 23% an issue in the semi-private sector (Whistleblowers Authority, 2016).

The **UK** Serious Fraud Office (SFO) recently updated its whistleblowing procedures to encourage greater reporting. In January 2016, the SFO launched a new website, introducing a "decision tree" reporting form that asks reporting persons a series of questions to try and establish at the outset whether their information should be supplied to the SFO (through the online secure reporting form) or to other UK agencies. To inform the public of this new reporting system, the SFO issued a statement referring to the new decision tree reporting form, although it did not actively seek to promote its use (UK SFO, 2012). The SFO press office also solicited feedback from stakeholders and journalists on the decision tree approach. The decision tree enables the SFO to redirect reporting persons to the appropriate government agency but the SFO considered that active promotion may have undermined that objective. The UK's Phase 4 evaluation notes that although the SFO received fewer tips following the introduction of the new system, the SFO received a greater number of relevant whistleblower tips.[4]

[4] UK Phase 4 Report (2017), paragraph 24, www.oecd.org/daf/anti-bribery/unitedkingdom-oecdanti-briberyconvention.htm.

Country practice: Reporting serious fraud, bribery and corruption	
United Kingdom Serious Fraud Office	"Whistleblowing is when an employee reports suspected wrongdoing at work. Officially this is called "making a disclosure in the public interest". If you suspect wrongdoing in your workplace, you should follow the whistleblowing procedures in your own organisation. If there aren't any or you are not comfortable reporting the matter internally there are a number of prescribed bodies to whom you can report in confidence. You can find useful advice on the Gov.uk website. The Serious Fraud Office is one of those prescribed bodies and we would like to hear from you if the wrongdoing concerns serious or complex fraud, bribery or corruption in a UK company. In such circumstances we would urge you to contact us using our secure reporting form." *Source: UK SFO website: www.sfo.gov.uk*

In **France**, in accordance with article 8 of the Loi Sapin II, reports must be made first internally "to the direct or indirect hierarchical superior, the employer or a person designated by the employer." Where this internal process is unsuccessful, the report can be addressed to a law enforcement authority, administrative authority or professional association. In cases of grave and imminent danger or where there is a risk of irreversible damage, the disclosure can be made directly to these organisations. As a last resort, and failing a response by the abovementioned organisations within three months, the report may be made public. The Loi Sapin II further requires public and private sector bodies with at least 50 employees to "establish appropriate procedures for receiving reports from members of their personnel or external and occasional collaborators." Finally, "any person can make his/her report to the Defender (*Défenseur des droits*)[5] to be directed towards the appropriate organisation to receive the report". Attempts to obstruct reporting or retaliate against those who report under the Loi Sapin II are punishable by one year's imprisonment and a EUR 15 000 fine.

Country practice: Whistleblower Hotline	
United States: Whistleblower Hotline, US SEC, Office of the Whistleblower	The OWB created a whistleblower hotline, in operation since May 2011, to respond to questions from the public about the SEC's whistleblower programme. Individuals leave messages on the hotline, which are returned by OWB attorneys within 24 business hours. To protect the identity of whistleblowers, OWB will not leave return messages unless the caller's name is clearly and fully identified on the caller's voicemail message. If OWB is unable to leave a message because the individual's name is not identified or if it appears to be a shared voicemail system, OWB attorneys make two additional attempts to contact the individual. During 2017, the Office returned nearly 3 200 phone calls from members of the public and has returned over 18 600 calls since the hotline was established. Many of the calls OWB receives relate to how the caller should submit a tip to be eligible for an award, how the Commission will maintain the confidentiality of a whistleblower's identity, requests for information on the investigative process or tracking an individual's complaint status, and whether the SEC is the appropriate agency to handle the caller's tip. *Source: US SEC, OWB Annual Report, 2017*

[5] The Defender (*Défenseur des droits*) is an independent constitutional authority. Nominated by the President for a six year mandate, the Defender is mandated to defend citizens' rights against the administration (ombudsman) but also has special prerogatives in the area of promoting the rights of children, the fight against discrimination and the respect of ethics and safety.

1.3 Provide guidance and follow-up

Whistleblowers take significant personal risks in reporting bribery and other crimes and misconduct to law enforcement authorities. Supporting and advising whistleblowers during the time they are deciding whether to make a report should help to instil confidence in the system and encourage reporting. For example, the US SEC's Whistleblower Hotline provides guidance to prospective whistleblowers about the SEC's whistleblowing programme. It can also be helpful for the support and advice to be provided by an independent third party. In this context, NGOs such as the Government Accountability Project (GAP), Public Concern at Work (PCaW), and Transparency International support, advise and accompany whistleblowers as they raise their concerns internally within their organisation or externally to law enforcement, the media, or other parties.[6]

Countries should consider whether it would be practical and helpful to encourage whistleblowing by instituting formal policies in their whistleblowing programmes that require periodic communication with whistleblowers about the status of their tip after it has been filed. A communication strategy could help to assure whistleblowers that their concerns are being heard and allow law enforcement authorities to ask follow-up questions to clarify or obtain further information. Such a strategy should also balance the need to keep information on ongoing investigations and proceedings confidential. **Austria**'s Ministry of Justice has established an innovative way of ensuring anonymity to whistleblowers, whilst enabling law enforcement authorities to obtain additional information to progress the case. In **Canada**, the Values and Ethics Code for the Public Sector sets out duties and obligations of senior officers for disclosure of wrongdoing, including to "[n]otify the person(s) who made a disclosure in writing of the outcome of any review and/or investigation into the disclosure and on the status of actions taken on the disclosure, as appropriate." [7]

[6] The Government Accountability Project (GAP) is a US whistleblower protection and advocacy organisation. A non-partisan public interest group, it litigates whistleblower cases, helps expose wrongdoing to the public, and actively promotes government and public accountability. Since 1977, GAP has helped over 6, 000 whistleblowers (www.whistleblower.org/); Public Concern at Work is a UK-based whistleblowing charity that advises individuals considering whistleblowing at work, supports organisations with their whistleblowing arrangements, informs public policy and seeks legislative change (www.pcaw.co.uk/); Transparency International has established Advocacy and Legal Advice Centres in more than 60 countries, which advise whistleblowers in making their disclosures and work to make sure that their disclosures are duly addressed by appropriate authorities (www.transparency.org/getinvolved/report).

[7] See: www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25049.

Country practice: Whistleblower Portal	
Austrian Federal Ministry of Justice	In 2013, the Federal Ministry of Justice in Austria launched a portal (www.bkms-system.net/wksta) to enable individuals to report wrongdoing. The portal can be also be accessed via a link on the Federal Ministry of Justice homepage (www.justiz.gv.at/web2013/html/default/2c9484853d643b33013d8860aa5a2e59.de.html), where individuals can find and download further information on the portal. The portal is operated by the Central Public Prosecutor's Office for Combating Economic Crimes and Corruption (CPPOCECC). The whistleblowing system is an online anonymous reporting system, which is especially suited for investigations in the area of economic crimes and corruption. The whistleblower (or "discloser") may report anonymously any suspicion that a crime in the general remit of the CPPOCECC pursuant to section 20a of the Code for Criminal Procedure (CCP) was committed; the investigation authority in turn may make inquiries with the whistleblower, while maintaining his or her anonymity in order to verify the value of the information. Any reports within the focus set forth by section 20a CCP, but outside the CPPOCECC remit, are forwarded to the competent authority (mostly financial authorities). To ensure that anonymity is guaranteed, when setting up a secured mailbox, the whistleblower is required to choose a pseudonym/user name and password. The anonymity of the information disclosed is maintained using encryption and other security procedures. Furthermore, whistleblowers are asked not to enter any data that gives any clues as to their identity and to refrain from submitting a report through the use of a device that was provided by their employer. Following submission, the CPPOCECC provides the whistleblower with feedback and the status of the disclosure through a secure mailbox. If there are issues that need to be clarified regarding the case, the questions are directed to the whistleblower through an anonymous dialogue. Such verified reports can lead to the opening of investigations or raise concrete suspicions requiring the initiation of preliminary investigations. As of 31 May 2017, the introductory page of the electronic whistleblowing system was accessed 343 0296 times. A total of 5 612 (possible) criminal offences were reported, less than 6% of which were found to be completely without justification. A total of 3 895 of the reports included the installation of a secured mailbox. About 32% of the reports fell into the scope of other (especially financial) authorities and were forwarded accordingly.The following description is available on the website in English and German: " … [P]rosecution offices and police usually also depend on the information of responsible citizens. Often individual persons shy away from divulging information due to their fear of personal disadvantages. The reasons for this can for example be the involvement of colleagues or superiors. Also the uncertainty of whether their information is taken seriously and investigated can be a problem. This protected communication platform serves to allay these doubts. Reports can be submitted anonymously and without being traceable. Please set up a secured postbox after reporting. This way, the prosecution office, unlike in the case of other anonymous reports, has the possibility to further establish the circumstances by directly asking you questions, in order to take appropriate and successful investigative measures. By using the provided communication platform you have the possibility to protect yourself by remaining anonymous and at the same time actively help in the clarification of economic crime and corruption ..." *Source: OECD, 2016a; Austrian Federal Ministry of Justice*

1.4 Consider financial rewards

There are currently two Parties to the OECD Anti-Bribery Convention that provide financial rewards to whistleblowers: **Korea** and the **United States**. Not only might financial payments incentivise whistleblowers to report information about misconduct, they can also provide financial support, such as living and legal expenses, following retaliation. Korea's Anti-Corruption and Civil Rights Commission (ACRC) is mandated under the Anti-Corruption Act and the Act on the Protection of Public Interest Whistleblowers (2011) to provide financial rewards to public and private sector whistleblowers who report internally within their organisation or directly to the ACRC. In addition, the Act permits whistleblowers to request compensation for their expenses, such as medical or psychological treatment, removal costs due to job transfer, and legal fees. In 2016, the Korean government amended the Act on the Protection of Public Interest Whistleblowers by, among other things, extending the scope of protected reporting and harmonising the financial rewards systems between the two laws. The ACRC paid KRW 10.5 billion (USD 9.38 million) for corruption reporting between 2012 and 2016, and KRW 2.64 billion (USD 2.35 million) for public interest reporting between 2011 and 2016.

To help expand the federal government's resources to detect misconduct in the securities industry, the Dodd-Frank Act authorises the US SEC to provide monetary awards to incentivise, compensate, and reward eligible individuals who voluntarily provide the SEC with original information that leads to a successful enforcement action that results in more than USD 1 million in sanctions. The range for awards is between 10% and 30% of the money collected. Factors that may increase an award percentage include the significance of the information provided by the whistleblower, the level of assistance provided by the whistleblower, the law enforcement interests at stake, and whether the whistleblower first reported the violation internally through the company's internal reporting channels. Since inception of the programme in 2011, the SEC has awarded more than USD 160 million to 46 whistleblowers and the SEC's enforcement actions from whistleblower tips have resulted in more than USD 975 million in total monetary sanctions, including more than $671 million in disgorgement of ill-gotten gains and interest, the majority of which has been, or is scheduled to be, returned to harmed investors (US SEC, 2017).

1.5 Ensure that criminal sanctions and civil defamation suits do not deter reporting

Criminal offences such as slander, violation of bank, commercial or professional secrecy, and corporate espionage can all be used to silence whistleblowers. In addition, civil defamation suits can have a chilling effect on whistleblowers seeking to speak up about wrongdoing in large, well-resourced organisations. Cases in **Russia and Switzerland**, where whistleblowers have been detained or held criminally liable for revealing wrongdoing detected in the course of their employment, highlight the need to strike a balance between punishing the malicious disclosure of sensitive corporate information and punishing those who speak out about possible misconduct that affects the public interest.[8]

[8] See, for example, Russia's Phase 2 Report, para. 42.

1.6 Ensure data protection legislation does not impede reporting

As noted in the OECD/G20 Study on G20 Whistleblower Protection Frameworks, data protection laws in some countries may impose legal restrictions on internal private sector whistleblowing procedures (OECD, 2012). The EU's General Data Protection Regulation (GDPR) and the EU Data Protection Directive (2016/680) will apply across all EU member countries from 25 May 2018. As company whistleblower reporting mechanisms rely on the processing of personal data (both of the reporting person and the subject of the report), the establishment of such reporting mechanisms will be subject to this strengthened data protection framework. This would mean that companies that have implemented, or intend to implement internal reporting mechanisms may need to obtain prior approval from national data protection authorities. Furthermore, companies could be liable to pay administrative fines amounting to the greater of EUR 20 million or 4% of total worldwide annual turnover should data protection authorities consider that companies' internal reporting mechanisms and subsequent internal investigation procedures violate GDPR provisions on data processing, data subjects' rights (i.e. the subject of the whistleblower report), or transfer of personal data to third countries or international organisations.[9] The requirement for prior approval of reporting mechanisms coupled with the risk of significant financial penalties could be major deterrents for companies considering whether to implement protected internal reporting channels.

Even before the entry into force of the GDPR, data protection laws have presented an obstacle to promoting whistleblower reporting mechanisms within companies. In **France**, courts have invalidated companies' internal whistleblowing procedures where the whistleblowing provisions were too broad in scope and could apply to actions which could harm the vital interests of the company, or physical or moral integrity of an individual employee; where the provisions did not sufficiently detail the rights of the individual subject of a whistleblowing complaint; or where there was a risk of slanderous reporting in the workplace.[10] In **Greece**, the Hellenic Data Protection Authority, in decision No. 14/2008,[11] declared a Greek company's internal whistleblower system illegal and sanctioned it for failing to abide by the regulations and procedures envisaged in Greek and EU data protections laws. As a result, those who reported under this system failed to qualify for protection and the monetary sanctions imposed on the company may have deterred other companies from setting up whistleblower systems. It is important for data protection regulators to be aware of the importance of promoting protected reporting within companies, whilst ensuring respect for data protection provisions. On the other hand, the GDPR's strengthened data protection provisions will ensure greater respect for the confidentiality of whistleblowers.

[9] GDPR, Article 83(5).

[10] See, for example, 8 December 2009 Decision of the French Cour de Cassation.

[11] 12-09-2008 – Απόφαση Αρ. 14/2008 - Επιβολή κυρώσεων στην εταιρεία ABBOTT LABORATORIES ΕΛΛΑΣ ΑΒΕΕ, www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=201,90,84,96,141,65,145,84.

Country practices: Data protection legislation and private sector reporting mechanisms	
Denmark	In its Phase 3 evaluation of Denmark, the WGB noted that despite the absence of private sector whistleblower protection legislation, Danish companies were increasingly adopting internal reporting mechanisms that had to be approved by the Danish Data Protection Agency (DDPA) to ensure compatibility with data protection laws. At the time of the evaluation in 2013, the DDPA had approved systems in over 100 companies. To further facilitate reporting, some companies provided measures to protect whistleblowers; however, in the absence of legal protection to whistleblowers against employment retaliation, these whistleblower mechanisms were judged to have limited effectiveness. The WGB recommended that Denmark promptly put in place public and private sector whistleblower protection measures. *Source: Denmark's Phase 3 Report (2013); OECD, 2016a.*
France	In France, courts have invalidated companies' internal whistleblowing procedures on the basis of data protection laws, including where the whistleblowing provisions were too broad in scope and could apply to actions that could harm the vital interests of the company or the physical or moral integrity of an individual employee. The Commission on Information Technology and Liberties (CNIL) has developed an expedited approval procedure whereby companies file a statement of compliance with the French data protection law (No. 78-17 of 6 January 1978). At the time of France's Phase 3 Written Follow-Up Report to the WGB in 2014, the CNIL estimated that 3 000 companies had a "professional whistleblower system".

2. How can whistleblowers be better protected against reprisals?

There is a significant legal disparity among Parties to the OECD Anti-Bribery Convention regarding the employment and post-employment protections available to whistleblowers. Several countries still provide only partial protection to whistleblowers through prohibitions against workplace harassment and unfair dismissal in labour laws. In some countries, protection of whistleblowers only applies in certain sectors (such as public officials, or in the financial sector). Only nine countries have enacted standalone, comprehensive whistleblower protection legislation that applies to employees in both the public and private sectors.[12] Member countries should consider whether harmonising their whistleblowing protections into a single, standalone legislative framework would improve the public's understanding of the of whistleblowing protections afforded to them and the mechanisms to enforce those protections. Elements to ensure the effectiveness of legislative frameworks for whistleblower protection are discussed below.

2.1 Protect whistleblowers who report internally as well as externally

The OECD 2010 Good Practice Guidance on Internal Controls, Ethics and Compliance recommends that companies ensure internal and, where possible, confidential reporting by and protection of whistleblowers who report breaches of the law or

[12] Hungary (Act CLXV. of 2013 on Complaints and Public Interest Disclosures); Ireland (Protected Disclosures Act (No.14 of 2014); Japan (Whistleblower Protection Act of 2004); Korea (Act on the Protection of Public Interest Whistleblowers of 2011); New Zealand (Protected Disclosures Act of 2000); Norway (Working Environment Act); Slovak Republic (Act No. 307/2014 Coll. on Certain Aspects of Whistleblowing); South Africa (Protected Disclosures Act 2000); United Kingdom (Public Interest Disclosure Act of 1998).

professional standards or ethics occurring within the company. Providing confidentiality and anti-retaliation protections to those who report internally within their organisation and those who report externally to law enforcement, the media or civil society is essential to a whistleblower protection framework.

The preponderance of evidence suggests that most whistleblowers report (or want to report) internally first. For example, of the private sector whistleblowers who have received financial rewards for reporting wrongdoing to the US SEC to date, approximately 83% first raised their concerns internally to their supervisors, compliance personnel, or through internal reporting mechanisms, or understood that their supervisor or relevant compliance personnel knew of the violations before reporting to the SEC (US SEC (2017). The US SEC has emphasised that "an individual who reports internally and suffers employment retaliation will be no less protected than an individual who comes immediately to the Commission."[13] Whistleblowers that are provided protected internal reporting can help companies learn earlier of wrongdoing and avail themselves of the opportunity to make an early self-report (where such mechanisms exist under national law), which in turn can lead to more expedient and efficient enforcement outcomes. An analysis of foreign bribery schemes noted that, of companies that self-reported bribery in their international operations to law enforcement authorities, 5% found out from a whistleblower. Furthermore, if whistleblowers report internally and no action is taken, they may feel more comfortable alerting law enforcement to their concerns if they know they are protected regardless of whether they reported internally first. Some countries require whistleblowers to report internally first in order to be protected against retaliation. External reporting is permitted in urgent cases, where no action is taken following the internal report or where there is "reasonable cause". This is the case, for instance, in **France**, **the Netherlands** and **Sweden**. [14]

External reporting should also be protected. Current OECD standards provide that public and private sector whistleblowers who report to external law enforcement authorities in good faith and on reasonable grounds should be protected against retaliation or discrimination. Although outside the current OECD standards for whistleblower protection, countries should consider providing protection to whistleblowers who report externally to the media or civil society organisations. As highlighted in Chapter 4 of this Study, responses to the OECD Survey on Investigative Journalism indicate that whistleblowers are the greatest source of information for journalists reporting on corruption cases. The need for greater protection of sources was raised in almost every response to the survey and whistleblower protection frameworks were the second-most valuable resource for journalists behind strong editorial support. It is important that potential whistleblowers are aware that in some countries only external reporting to relevant law enforcement authorities is protected, and reports made to the media or civil society will not necessarily receive follow up or be protected from reprisals. In **Canada**, the Journalistic Sources Protection Act, which was assented to on 18 October 2017, amends the Canada Evidence Act and the Criminal Code to confer further protections for the confidentiality of journalistic sources.

[13] Interpretation of the SEC's Whistleblower Rules Under Section 21f of the Securities Exchange Act of 1934 [Release No. 34-75592], US SEC, www.sec.gov/rules/interp/2015/34-75592.pdf.

[14] In Sweden it is only the case for employees in the private sector. Employees in the public sector are protected regardless of whether they report internally first. External reporting is permitted regardless the cause.

2.2 Define reporting persons and protected disclosures broadly

In any whistleblower protection framework, it is important to clearly identify the types of employment arrangements that benefit from protected reporting. With respect to categories of protected "reporting persons," definitions must go beyond the traditional employment relationship to include consultants, contractors, trainees/interns, temporary employees, former employees, volunteers, and employees of state-owned or controlled enterprises and statutory agencies. In the context of foreign bribery reporting, it is also essential that protection extend to foreign or overseas-based employees. A broad range of disclosures should also be afforded whistleblower status and protections. Whistleblowers should not be required to categorise the nature of the wrongdoing they report, such as identifying the specific laws that might have been violated or whether the possible misconduct constitutes a crime. Thus, the protected reporting should not be restricted to the particular subject matter of the report. Recognising that segregating corruption from other kinds of public interest reporting deterred potential whistleblowers from reporting, Korea amended its Act on the Protection of Public Interest Whistleblowers to harmonise the protection frameworks and extend the number of laws covering public interest from 180 to 279. The Canadian Public Servants Disclosure Protection Act protects against a broad range of "wrongdoings" in, or relating to, the public sector (see s.8 PSDPA). Whistleblowers are only required to make a disclosure in good faith that they believe could show a wrongdoing. They are not required to categorise the nature of the wrongdoing.

As discussed above, criminal and civil sanctions for frivolous and defamatory reporting, or requirements that the report be made "in good faith", can deter whistleblower reporting. Even disgruntled employees, or employees actually involved in the wrongdoing, may become genuine whistleblowers and should also be entitled to protection. The UN Office on Drugs and Crime (UNODC) Technical Guide to the United Nations Convention against Corruption (UNCAC) states that "good faith should be presumed in favour of the person claiming protection, but where it is proved that the report was false and not in good faith, there should be appropriate remedies" (UNODC, 2009, p.107). The **UK** adopted this position in 2013 when it amended certain provisions in the Public Interest Disclosure Act (PIDA), notably to replace the good faith-requirement with a less onerous public interest test, thus shifting the focus of the legislation "from the messenger to the message".[15] In **New Zealand**, the motive of the person reporting wrongdoing is not relevant, but the Protected Disclosures Act 2000 (PDA) requires that the employee must believe on "reasonable grounds" that the information about suspected serious wrongdoing is true or likely to be true for the disclosure to come within the act and its protections (OECD, 2016a, p.51). **Ireland** omitted the public interest test from its Protected Disclosures Act 2014, deeming it a potential obstacle for individuals to come forward and acknowledging that in practice it may be difficult to distinguish what could qualify as a matter of public interest. As a result, the measures in place in Ireland reflect the notion that the public interest involved in attracting genuine whistleblowers far outweighs the public interest in seeking to punish persons who may report allegations in bad faith (OECD, 2016a, p.52).

[15] United Kingdom's Phase 4 Report (OECD, 2017), para. 29, www.oecd.org/daf/anti-bribery/unitedkingdom-oecdanti-briberyconvention.htm. It should be noted, nevertheless, that bad faith reporting may lower compensation by 25%.

2.3 Ensure anonymity or confidentiality

A fundamental method to protect and encourage whistleblowers is to ensure that they can make anonymous or confidential reports. However, anonymous reporting is not a substitute for robust anti-retaliation protections because the identity of the whistleblower could be deduced from the content or circumstances of the disclosure, such as reporting in small companies or small countries. From a practical perspective, it is also difficult to provide comprehensive protection to a person whose identity is unknown but that could be deduced by potential retaliators for the reasons described above. Anonymous reporting also makes it difficult to obtain additional information from the reporting person that might be essential to understand and remediate the wrongdoing and could have the unintended consequence of generating false or vindictive allegations if the reporting person cannot be identified and held accountable. The US SEC allows whistleblowers to make anonymous reports if they are represented by a lawyer but requires whistleblowers to disclose their identity before the SEC will pay them an award (Rule 21F-7). Since inception of the programme in 2011, 19% of the whistleblowers who received a financial reward from the SEC submitted their information anonymously through legal counsel (US SEC, 2017). As illustrated above, the Austrian Ministry of Justice uses an external service provider for its reporting platform, which enables encrypted anonymous reporting and follow-up and feedback through a case numbering system.

Whistleblowing laws should forbid the disclosure of the whistleblower's identity (or any information that could reveal the whistleblower's identity), and clearly state the exceptions to this principle that would require the whistleblower's identity to be revealed. For example, in the US, one of the exceptions in SEC Rule 21F-7 permits the SEC to disclose a whistleblower's identity, when the SEC brings litigation against an alleged wrongdoer in federal court or in an administrative proceeding, and the whistleblower is called as a witness in the proceeding. In this circumstance, the defendant may have the right to know that the witness is a whistleblower and therefore has a potential financial interest in the outcome of the matter. On the other hand, to the extent that a whistleblower becomes a witness in a criminal trial, they may benefit from additional protection under witness protection provisions available in most countries.

Member countries should also consider ways to ensure the confidential handling of whistleblower reports and the whistleblower's identity. For example, confidentiality can be enhanced by exempting whistleblower reports from disclosure under freedom of information legislation (e.g. **Italy's** access to information law has an exception for public employees reporting offences, as does its new whistleblower protection law).[16] In addition, disciplinary provisions for breach of confidentiality requirements (and enforcement thereof) can boost whistleblower confidence in reporting mechanisms. In Korea, disclosure of a whistleblower's identity, or facts that may infer it, is punishable by 3 years imprisonment or a fine of KRW 30 million.[17]

In **France**, "procedures for receiving reports must guarantee strict confidentiality of the identity of the reporting persons, persons the object of the report and the information collected by all recipients of the report" (art.9 Loi Sapin II). Elements that could identify

[16] Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o private, approved by the Italian parliament on 15 November 2017.

[17] Act on the Protection of Public Interest Whistleblowers, Chapter V Article 30 (1).

the whistleblower may not be disclosed except to law enforcement authorities and only with the consent of the whistleblower and once the report has been substantiated. The disclosure of confidential information is punishable by two years' imprisonment and a EUR 30 000 fine."

2.4 Financial compensation and other protections

As mentioned above, **Korea**'s whistleblower protection framework provides for financial rewards: in cases of internal whistleblowing which has led to direct recovery or increase of revenue of central or local governments, awards can range from 4-20% of the assets recovered up to KRW 2 billion; or up to KRW 20 million in cases of whistleblowing which contributed to upholding the public interest or prevented losses to, or led to pecuniary advantages for, central or local governments. Korea also has a financial compensation system to cover whistleblowers' expenses, such as medical expenses, removal expenses due to job transfer, legal costs and loss of wages. The ACRC can also order emergency police protection in cases of threats to physical safety. It has negotiated MOUs with the Korean Neuro-Psychiatric Association to provide financial support for psychiatric treatment of whistleblowers and with the Korean Bar Association to provide legal aid to whistleblowers. The UK PIDA also provides for compensation for the full financial losses of those found to have been unfairly dismissed. The level of compensation for full financial losses is uncapped, although the circumstances under which they are paid will depend on the facts of each case. The UK (HM Courts and Tribunals Service) does not maintain publically available or centrally held date on individual rewards.

In **Canada**, an individual who is the subject of an act of reprisal (including demotion, termination of employment and any other action or threat that adversely affects employment of working conditions) can make a complaint to the Integrity Commission, which may lead to a financial settlement. Sections 738 to 741.2 of the Criminal Code govern restitution orders as part of the sentencing process (including for the offence of retaliating against an employee who has provided information to law enforcement authorities about an offence committed by their employer, or to prevent an employee from so doing). Section 738 authorises a stand-alone restitution order to cover costs including for loss, destruction or property damage as a result of the commission of an offence and all readily ascertainable pecuniary damages, including loss of income or support, to any person who has suffered bodily or psychological harm from the commission of an offence. Restitution may also be ordered as a condition of a probation order or of a conditional sentence.

2.5 Sanctions for retaliation

Whistleblower protection systems need to contain measures to protect against reprisals if confidentiality mechanisms fail and the employer deduces the whistleblower's identity, thereby creating a risk of retaliation by the employer or other employees. Sanctions for reprisals against whistleblowers must consider the full range of retaliatory and discriminatory conduct. Examples of retaliation include, but are not limited to dismissal, demotion, reassignment of roles or tasks, denial of education, training or self-promotion opportunities, bullying, violence or unfair audit of the person's work. Whistleblowers should also be protected against threats of reprisals. Most Parties to the OECD Anti-Bribery Convention with whistleblower protection legislation provide

protection for a broad range of reprisals, with penalties ranging from disciplinary action to fines and imprisonment.

Box 2. **United States Case Study: International Game Technology (IGT) (2016)**

On 29 September 2016, the SEC brought its first stand-alone retaliation case under Section 21F(h)(1) of the Exchange Act. The whistleblower, a director of a division of casino gaming company International Game Technology (IGT), had received positive performance evaluations throughout his tenure with the company, including his mid-year review in 2014. Shortly after the whistleblower received a favourable 2014 mid-year review, the whistleblower raised concerns to senior managers, to the company's internal complaint hotline, and to the SEC that IGT's publicly reported financials may have been distorted. The whistleblower became concerned that the company's cost accounting model could result in inaccuracies in IGT's financial statements and reported these concerns to management and the SEC. Within weeks of raising the concerns, the whistleblower was slated for termination and removed from significant work assignments. The company conducted an internal investigation into the whistleblower's allegations and determined that its reported financial statements were not inaccurate. Shortly thereafter, IGT fired the whistleblower. The SEC found that IGT's conduct violated Section 21F(h), and IGT agreed to pay a USD 500 000 civil penalty to settle the charges.

Source: US SEC OWB Annual Report 2016; In the Matter of International Game Technology, Rel. No. 78991, File No. 3-17596 (Sept. 29, 2016)

Criminal sanctions are perhaps the most dissuasive form of penalty for reprisals. The **US** Federal Criminal Code 18 USC. §1513 (e) states that "whoever knowingly, with the intent to retaliate, takes any action harmful to any person, including interference with the lawful employment or livelihood of any person, for providing to a law enforcement officer any truthful information relating to the commission or possible commission of any Federal offense, shall be fined under this title or imprisoned not more than 10 years, or both." In 2004, the Criminal Code of **Canada** was amended to introduce a crime of retaliation applicable to all employers and employees in Canada and punishable by a maximum of 5 years' imprisonment. It provides that "no employer or person acting on behalf of an employer or in a position of authority in respect of an employee of the employer shall take a disciplinary measure against, demote, terminate or otherwise adversely affect the employment of such an employee, or threaten to do so, **(a)** with the intent to compel the employee to abstain from providing information to a person whose duties include the enforcement of federal or provincial law, respecting an offence that the employee believes has been or is being committed contrary to this or any other federal or provincial Act or regulation by the employer or an officer or employee of the employer or, if the employer is a corporation, by one or more of its directors; or **(b)** with the intent to retaliate against the employee because the employee has provided information referred to in paragraph (a) to a person whose duties include the enforcement of federal or provincial law."

Civil and administrative penalties can also be effective to dissuade employers from retaliating against their current or former employees who blow the whistle or assist a government's prosecution. For example, in the United States, Section 21F(h)(1)(A) of the Securities Exchange Act authorises the SEC to seek civil penalties against employers that engage in a wide-range of retaliatory actions against whistleblowers who report possible misconduct to the SEC or assist in an SEC investigation, judicial or administrative action; or in making disclosures required by other laws. Pursuant to whistleblower protection legislation that entered into force in Sweden in January 2017, employers who retaliate

against whistleblowers are required to pay damages. The burden of proof rests on the employer to demonstrate that the retaliation did not occur.[18] **Korea**'s ACRC has a range of powers available to sanction companies for whistleblower reprisals, including ordering reinstatement of whistleblowers who have been transferred, demoted or fired. In a recent high-profile whistleblower case, Hyundai accepted ACRC recommendations to reinstate a former general manager who was fired after reporting information about vehicle defects to the Korean government, which resulted in product recalls. Hyundai filed an administrative lawsuit disputing the validity of the initial termination, but withdrew the lawsuit in May 2017.[19] Norway's Phase 3 evaluation highlights the effectiveness of Norway's whistleblower protection systems in the context of one company at the on-site visit, which explained that the employee who blew the whistle on the suspicions of foreign bribery that subsequently led to the company's conviction for the offence was still employed with the company.[20]

2.6 Civil remedies for whistleblowers

An additional form of protection is to provide private rights of action to aggrieved whistleblowers to sue the company or individual managers or directors for damages as a result of the discriminatory or retaliatory behaviour. Civil damages help compensate whistleblowers who have been fired and have difficulty finding future employment and could include lost income and litigation costs, such as attorney's fees. In the United States, the Sarbanes-Oxley and Dodd-Frank Acts provide such private rights of action. **Bulgaria**'s Conflict of Interest Prevention and Ascertainment Act provides, in art. 32(4), that "a person, who has been discharged, persecuted or in respect of whom any actions leading to mental or physical harassment have been taken by reason of having submitted a request, shall have the right to compensation for the personal injury and damage to property according to a judicial procedure."

[18] Act on special protection against victimisation of workers who sound the alarm about serious wrongdoings (2016:749).

[19] Hyundai Motor to reinstate whistleblower who leaked info about recall coverup, 30 April 2017, The Hankyoreh (see: http://english.hani.co.kr/arti/english_edition/e_business/792836.html).

[20] Norway's Phase 3 Report (2011), para. 105, www.oecd.org/daf/anti-bribery/norway-oecdanti-briberyconvention.htm.

Box 3. **United States Case Study: Wadler v. Bio-Rad Laboratories, Inc. (2017)**

For 25 years, Sanford Wadler was general counsel at Bio-Rad Laboratories, Inc., a Fortune 1000 company that manufactures and sells products and equipment around the world. In 2009, Bio-Rad's management became aware that its employees may have violated FCPA provisions in Vietnam, Thailand, and Russia. The company hired a law firm to investigate whether employees were engaging in bribery in China. The firm concluded that there was no evidence of improper payments. However, in 2011, Wadler discovered no documentation supporting Bio-Rad's significant sales in China and was concerned that this constituted a violation of FCPA books and records requirements and possible concealment of bribes. In 2013, he learned that standard language on the need for FCPA compliance had been removed without his knowledge or approval, from documents translated into Chinese for use in Bio-Rad's operations in China. He brought these concerns to the attention of the Audit Committee and the company's external lawyers and accountants. On 7 June 2013, Sanford Wadler was fired.

Sanford Wadler filed a complaint of termination for engaging in protected activity with the Department of Labor, in accordance with the requirements of the Sarbanes-Oxley Act. He subsequently filed a suit against Bio-Rad and the individual members of its board of directors in the Northern District of California in May 2015. On 6 February 2017, a Federal Jury found that Bio-Rad Laboratories, Inc. would not have terminated Wadler had he not reported these allegations to the Audit Committee. The jury awarded Wadler nearly USD 11 million in damages; USD 2.96 million in back pay, doubled under the Dodd-Frank Act, in addition to USD 5 million in punitive damages. This award is one of the highest civil damages awards to a US whistleblower, to date. The jury found that Bio-Rad's wrongful conduct involved malice, oppression or fraud, entitling Wadler to punitive damages. This finding appears to be based on Bio-Rad's submission into evidence of a negative performance review for Wadler that, while dated April 2013 (prior to Wadler's termination), was shown in metadata to have been created in July 2013 (after his termination). In an earlier interlocutory judgment in the same case, the court confirmed the SEC's interpretation of the Dodd-Frank Act; that its anti-retaliation provisions extend to internal reports of wrongdoing. The court also importantly found that corporate directors of public companies can be held individually liable for retaliating against a whistleblower. Bio-Rad has appealed the verdict.

Source: Wadler v. Bio-Rad Laboratories Inc. et al., case number 3:15-cv-02356, in the US District Court for the Northern District of California

Conclusion

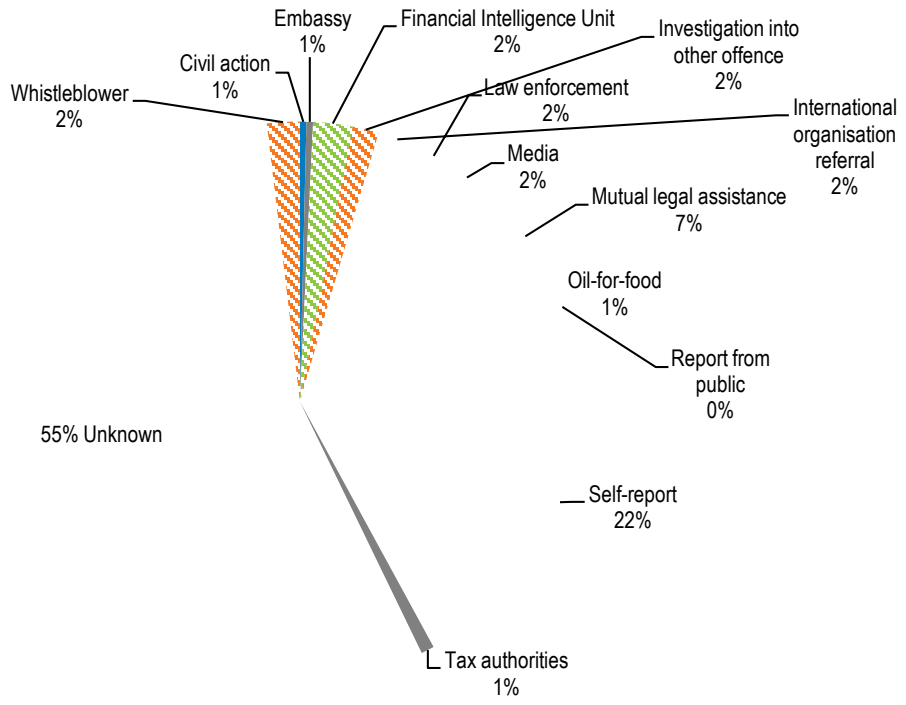
Whistleblowers must have effective legal protection in the form of guaranteed confidential reporting and anti-retaliation protections to freely and safely report suspected bribery of foreign public officials. The WGB continues its rigorous monitoring of countries' frameworks to protect private and public sector employees who report suspicions of foreign bribery. While several countries have recently enacted whistleblower protection legislation, two-thirds of Convention Parties still do not provide satisfactory protection. Given the importance of whistleblowers as a source of detection in foreign bribery cases, the WGB will monitor this issue as a priority in the Phase 4 country evaluations.

Annex. 1 Scope and Methodology of the OECD study on The Detection of Foreign Bribery

The study looks at primary sources of detection for the foreign bribery offence, that is to say at the role that certain public agencies – other than law enforcement – or private sector actors can play in uncovering foreign bribery. The detection sources examined in the ten chapters of this study have been identified on the basis of (1) their recurrence as a source of detection in foreign bribery cases (e.g. self-reporting), (2) the standards in the OECD Anti-Bribery Convention and 2009 Recommendation on Further Combating Bribery of Foreign Public Officials in International Business Transactions (the 2009 Recommendation), which identify certain agencies or professionals as playing a particular role in the detection of foreign bribery (e.g. whistleblowers, foreign representations, tax authorities, external auditors), and (3) more recent trends which point to an evolving role in the foreign bribery context (e.g. the legal profession, or competition authorities).

Each of the ten chapters identifies the number of foreign bribery cases detected through each source (see Figure 1, and data collection methodology). Recalling the relevant standards under the OECD Anti-Bribery Convention and related OECD anti-bribery instruments where applicable, each chapter then reviews available country practices developed in respect of the public agency or private sector actor concerned, and includes case studies based on finalised (or sometimes ongoing) foreign bribery cases to illustrate how, in practice, foreign bribery can and has been detected by the source in question.

Figure 1. **How are foreign bribery schemes detected? 1999-2017**



Source: OECD database on foreign bribery case

Each chapter has been developed under the mentorship of one or two country experts from the WGB, who provided their invaluable knowledge and guidance on the detection source. It builds on the over 200 country evaluation reports covering the 43 Parties' foreign bribery laws and enforcement practices and activities published by the WGB. Additional information provided by the countries, in the form of real-life case studies or description of practices, further illustrates what can be achieved to fully tap into the potential of certain sources. Finally, relevant experts have been consulted on specific sections of the report, including from the OECD as well as external stakeholders.

Data collection methodology

The study relies on data collected to identify detection sources for foreign bribery cases (or schemes) concluded between the entry into force of the OECD Anti-Bribery Convention in 1999 and 1 June 2017. A foreign bribery scheme encompasses one set of facts involving bribery of a foreign public official in an international business transaction, for which there may have been enforcement actions against several natural and/or legal persons. The data on detection sources extracted for the purpose of this study is the result of an analysis of 263 foreign bribery schemes which have been investigated, prosecuted and reached a final law enforcement outcome for the specific crime of bribery of foreign public officials in international business transactions, as set out in Article 1.1 of the OECD Anti-Bribery Convention and transposed into Parties' domestic legislation. Preparatory and participatory offences such as conspiracy, attempt, aiding and abetting foreign bribery are also included. The data collection does not, however, include foreign bribery-related offences (such as accounting and auditing, money laundering, trafficking in influence, fraud, commercial bribery, violation of duty of supervision, failure to prevent bribery) nor United Nations (UN) sanctions violations or other economic crimes.

The data collection is based on research into enforcement actions from countries Party to the OECD Anti-Bribery Convention, collected notably from court decisions and settlement agreements available on the websites of national law enforcement authorities; information provided by national authorities in the context of Phase 3 and 4 and follow-up evaluations by the WGB and following bilateral requests by the OECD Secretariat. The data was further verified by the countries Party to the OECD Anti-Bribery Convention. 0% values are when there are only 1 or 2 cases in the category. Furthermore, case information was not always complete, which explains the frequent "unknown" value on the sources of detection (see Figure 1). Due to the confidential nature of some of the information provided by national authorities, the study presents essentially aggregate figures, relying, where possible, on case studies for a more concrete illustration.

Annex. 2 Key Findings of the OECD study on The Detection of Foreign Bribery

In many respects, the OECD study on The Detection of Foreign Bribery demonstrates that a number of potential detection sources under review are largely untapped, and that much could be done by OECD Anti-Bribery Convention Parties to improve the use of these sources to improve detection of foreign bribery. The study and supporting data also show that detection of foreign bribery is a complex process, involving many potential sources, which can make it difficult to identify which source initiated the case. One case may have been detected by the media in one country, leading its law enforcement authorities to seek mutual legal assistance, thereby alerting authorities in a second country, and/or possibly triggering a report by a confidential witness or informant.

Naturally, adequate legal and institutional frameworks are the first step to promote detection by a given source. While each chapter of the study goes into the specificities applicable to each sector under review, it is generally true that clear and adequate protection, incentives and support (depending on the detection source) need to be afforded to those who report. Establishing and publicising reporting channels is also essential if any alleged foreign bribery that has been detected is to be reported to law enforcement authorities. Generally speaking, a broad approach is also preferable to encourage people to come forward if they suspect any kind of economic or financial misconduct: initial suspicions by non-experts may be more akin to sensing that "something is wrong", than to a specific determination that foreign bribery has occurred. Law enforcement may often be better placed to determine whether or not reports merit further investigation, and placing the onus to determine whether a set of facts is foreign bribery on persons whose profession is not to investigate and prosecute foreign bribery may be counterproductive.

In many instances, awareness and training are also key to detection. This goes well beyond alerting public officials or certain private sector actors of the existence of foreign bribery – foreign bribery is no longer a "new" offence in most Convention countries. When developing rigorous, profession-specific awareness-raising and training initiatives, authorities highlight the importance they give to fighting foreign bribery, and to the role that the targeted agency or profession can play in uncovering it. Training and guidance need to be tailored to the specific public agency or profession: each agency, each profession has a specific mission, and some of the red flags for detecting foreign bribery from their perspective will be unique to each. There can be no one-size-fits-all approach in this respect. Feedback from law enforcement following a report will also be important in developing the capacity to detect: it is a way of acknowledging the role played by the person or body in uncovering the foreign bribery. Where the detection source is a public agency or professional body, providing feedback also builds trust, increases expertise and mutual understanding, and more generally establishes a common goal of fighting bribery and corruption.

The study reviews a wide range of potential sources for detecting foreign bribery, analysing and explaining how detection mechanisms operate across ten subject areas and how these can lead to identifying potential foreign bribery. Nevertheless, by it very broad nature, the Study just skims the surface on a number of issues. As Convention countries and the WGB further develop their expertise on the topic of detection, and as public agencies, private sector actors and non-governmental organisations increasingly turn their attention to the topic of transnational bribery, additional research may be warranted. The WGB may therefore engage in greater depth with certain agencies or professions, with a view to deepen its understanding of how they function and how they may assist in detecting foreign bribery through their particular lenses.

The detection of foreign bribery poses a constant challenge to law enforcement authorities as neither the bribe payer nor the bribe recipient has any interest in disclosing the offence. Contrary to many other offences, there is rarely an easily identifiable, direct victim willing to come forward. The Detection of Foreign Bribery looks at primary detection sources which have been, or could be expected to be, at the origin of foreign bribery investigations. It reviews the good practices developed in different sectors and countries which have led to the successful detection of foreign bribery with a view to stepping up efforts against transnational bribery. This document reproduces Chapter 2 of the study on the role of whistleblowers and whistleblower protection in the detection of foreign bribery.

www.oecd.org/corruption