ENFCO

European Network for Compliance Officers

WHITEPAPER

THE ENFCO WHISTLEBLOWING FRAMEWORK

Navigating Challenges, Protection, and Best Practices

Report Date: June 23, 2026

Contents

A. ENFCO

ENFCO is a network of not-for-profit associations for in-house compliance professionals across Europe. The organization facilitates the cooperation and communication between the participating associations and their incorporated professionals in the best spirit of a European Community, according to the network's mission goals.

At the time of publication, the following Compliance Association (listed alphabetically) are members:

- AICOM (Associazione Italiana de Compliance) (Italy)
- ALCO - Association of Luxembourg Compliance Officers (Luxembourg)
- ASCO (Association of Compliance Officers) (Greece)
- ASCOM (Asociacion Espanola de Compliance) (Spain)
- BAAFC experts (Bulgarian Association of Anti-Financial Crime Experts) (Bulgaria)
- BCM (Berufsverband der Compliance Manager) (Germany)
- Le Cercle de la Compliance (France)
- Cercle d'Ethique des Affaires (France)
- Céská Compliance Asociace (Czech Republic)
- Compliance Hub (Kazachstan)
- Compliance Institute (Ireland)
- Compliance Pro (Belgium)
- Cumplen (Spain)
- Cyprus Compliance Association (Cyprus)
- Ethics and Compliance Switzerland (Switzerland)
- EICE (European Institute for Compliance and Ethics) (Slovenia)

- GACO (Gibraltar)
- GACO (Guernsey)
- Hrvatska Udruga Za Usklađenost Poslovanja - Croatian Compliance Association (Croatia)
- Hungarian Corporate Compliance Society (Hungary)
- Nordic Business Ethics (Scandinavia)
- OCOV (Austria)
- Portuguese Observatory and Regulatory (Portugal)
- Slovak Compliance Association (Slovakia)
- SSCE Montenegro
- VCO (Vereniging Compliance Officers) (Netherlands)

More information about ENFCO can be found on its website https://www.enfco.eu/

B. Summary of Interview with Pav Gill

Below you find a condensed summary of the interview conducted by Patrick Wellens (Chairperson Ethics and Compliance Switzerland) and Carlos M Martins (Chairperson Gibraltar Association of Compliance Officers) in representation of ENFCO (The European Network for Compliance Officers) on the 22nd of April 2026. The full interview is found in the appendix T.

Pav Gill (PG) is a Singaporean lawyer and entrepreneur, best known as the whistleblower who exposed the Wirecard scandal, one of the largest corporate frauds in European history. For his bravery and commitment to ethics, he has received numerous accolades, such as the **ACFE Cliff Robertson Sentinel Award** and the **Blueprint for Free Speech Special Recognition Award**. He is now a prominent keynote speaker on corporate governance and integrity.

Whistleblowing perception

PG: “What worries many employers is the fact that the employee went outside the organization. Many still see these matters as internal. Once someone goes to a regulator, the press or an outside lawyer, that person is often viewed as a red flag. That is where the idea of 'once a whistleblower, always a whistleblower' comes from.

There are exceptions. A regulated firm or a company that is serious about governance may see that background as a strength. They may want a lawyer, compliance officer or auditor who has lived through a major failure and knows where the red lines are.

That said, the ideal case is still the minority. In practice, many companies remain wary because they fear the issue will leave the building.

PG: “Part of the problem is that the term 'whistleblowing' is now used far too broadly. Sometimes the person is not exposing a criminal scheme at all. They are raising an operational risk, a control failure or something that simply does not add up.

I think of it as a hierarchy of reporting:

1. Whistleblowing: systemic, serious or potentially criminal issues.
2. Grievances: personal or workplace complaints.
3. Disclosures: raising a concern that may not be misconduct but still needs attention.

Companies need environments where people can ask questions or raise concerns without immediately being treated as adversarial. Spotting a discrepancy in an invoice does not mean the company is fraudulent. It may be a mistake. The issue is whether people feel safe enough to raise it.

That is why employability and reputation always come back to facts, context and how the next employer reads the situation."

Incentives to report misconduct

PG: "I am generally wary of legal structures that pull people straight out of the company and into the hands of the authorities. The US model creates a strong pull factor through financial incentives. Other systems have the opposite problem and make internal reporting almost pointless.

Take Malaysia. If the first person you speak to is not an enforcement agency, you can lose protection. I do not like that approach. Companies should have the chance to address an issue internally first, provided the internal channel is safe and credible. That takes you back to first principles: is the report anonymous, is there real protection of anti-retaliation and does the company actually walk the talk?

Most whistleblowers are trying to discharge a burden. They see something that does not make sense and want to report it so it can be dealt with. The problem begins when the company turns the reporter into the issue. That is when people start looking outside.

Financial reward is not the core driver in my view. A reward may make sense in certain public-interest cases, especially where public funds are involved, but whistleblowing should not be built around payout culture."

Trust in whistleblowing channels

PG: "It usually comes down to two things. First, can the person trust the channel? If the system sits on the company's own network and IT can work out who filed the report, anonymity is already compromised.

Second, does the company do anything once a report comes in? Outcome matters. When people see that a report led to a real investigation and a real sanction, even against someone senior, they start to trust the process.

So, the answer is safety first, then execution. If either is missing, people lose faith very quickly."

Malicious Reporting

PG: "The fear of malicious reporting is usually overstated. A report is only as strong as the evidence behind it, so weak or bad-faith allegations are often easy to filter early.

From the company's perspective, more information is usually better than less. Something that looks minor today may become important later when you see the broader pattern. The real challenge is not volume. It is handling.

You must go back to first principles. Can the allegation be substantiated? It is also critical to separate performance from conduct. Someone may be lawfully dismissed for poor performance and still have a legitimate complaint about harassment or abuse by a manager.

To manage the "grey zone" of post-termination reports, companies should adopt a dual-track approach to ensure both legal compliance and ethical integrity.

- **Track 1: The Performance Case:** Was the termination or redundancy based on objective, documented business needs or performance metrics? If yes, the company's legal position regarding the dismissal remains intact.
- **Track 2: The Conduct Case:** Regardless of the employee's performance, did the alleged misconduct occur? This investigation focuses on the accused party and the company's culture.
- **The Intersection:** Investigators must determine if there is a causal link—i.e., was the "poor performance" actually a result of the employee rebuffing the manager's advances?"

Compensating whistleblowers for emotional stress and financial loss

PG: "I am cautious about adding broad new financial burdens on companies. The practical problem with most compensation models is that they usually assume the whistleblower has identified themselves. You cannot reimburse someone or compensate them if you do not know who they are.

That takes you straight into questions of quantum, proof and years of litigation. Once you widen it beyond legal fees, the model becomes very hard to administer fairly.

A narrower legal-fees model is easier to defend. If a whistleblower gets legal advice and a credible claim of retaliation is established, there may be a case for a central fund to reimburse the legal work. That is far simpler than speculative payout models tied to recovery. If you base compensation on recovered funds, what happens when there is no recovery even though the retaliation was real? You create another layer of dispute.

My view is that the more urgent job is to audit and enforce company processes properly. The EU Directive was a good start, but enforcement is uneven. Spain can impose fines up to €1 million. Germany's maximum fine is €50,000. For a large company, that is not a meaningful deterrent. Until the stick is real, the framework will remain too easy to ignore."

Anonymity

PG: "Technical anonymity has limits. If only two or three people know a set of facts, the company may work out who reported it regardless of how strong the encryption is.

That is why I tell whistleblowers to build a careful chronology. Record when you reported who had access to the issue and what changed afterward. In the EU, where the burden of proof has shifted in retaliation cases, that timeline can be very powerful.

In most cases, I tell people to work backwards from the outcome they want before they do anything.

- Do you want to expose the company publicly?
- Do you want compensation for dismissal or retaliation?
- Do you want to trigger regulatory action?
- Or do you simply want to discharge the burden, sleep at night and move on?

Once you know the 'why', you can build a strategy around it and reduce avoidable risk."

Trust in company whistleblowing policies and procedures

PG: "I am deeply skeptical of the traditional hotline or outsourced call-center model. More than 95% of the people who contact me on LinkedIn are senior employees: CFOs, managing directors, heads of department. They are not going to discuss serious fraud with a random third-party call handler who does not understand the business.

The model also creates obvious risks:

- Translation risk: sensitive information may be pushed to third-party translators who should never see the case.
- Routing risk: we have already seen cases where reports were sent straight back to the people being accused.

I am equally wary of companies that have nothing more than a policy document and a shared email address. In those setups, you do not know who is behind the screen or who can access the data.

If I were assessing an employer, I would focus on two things:

1. Independent oversight: the case managers should report at a level that can actually hold management to account, ideally through the audit and risk structure or the board.
2. Secure infrastructure: the company should have a dedicated platform rather than a paper policy and a hope that nobody misuses the inbox."

Artificial Intelligence

PG: "AI can help or hurt. It depends entirely on how it is deployed and governed.

If the system is ring-fenced, transparent and not exposing data to third parties, AI can improve the front end. An AI interface may be better than an outsourced call center because it does not judge the reporter. It can capture the basics and flag urgent cases, such as self-harm or possible criminal activity. It should not be giving legal advice.

The first reporting stage is where many people drop off because the process is too long or too clumsy. AI can help through conditional logic. For example, if someone in construction or healthcare reports an injury, the system can immediately ask the right follow-up questions while the reporter is still engaged.

It also has a role on the backend in producing reports for boards, auditors and regulators, and in helping organizations meet feedback obligations under the EU Directive. The key is disclosure. People need to know how AI is being used and where its role stops."

Psychological safety

PG: "I am not a psychologist, so I would not pretend to solve the culture piece in a neat slogan. In practice, a safety net depends on two things: the whistleblower has identified themselves and the company wants to act in good faith.

Once a real investigation is underway, there are practical protections available. That may mean gardening leave, moving the person out of a hostile reporting line or creating some other safe environment while the investigation runs.

But the most important discipline is simpler than that. When a report arrives, the first question should never be, 'Who is this person and why are they saying this?' If you start there, you are already moving away from the facts.

The better question is: even if this came from an alien, is it true, and would ignoring it harm the company? If the answer is yes, act on the substance first. Motive and identity can wait."

Whistleblowers seen as troublemakers

PG: "From a governance perspective, boards are the ones on the line when things go wrong. Their basic question should always be: 'What did we do to prevent this?'

A lot of resistance comes from the view that most reports are malicious or merely employee grievances. Even if that were true, it is not a reason to dismiss the channel. A board that sees whistleblowing as an inconvenience is itself a red flag.

Technology helps, but tips still matter. The ACFE has found that 43% of occupational fraud is detected through tips. That is a huge part of the risk picture.

If a board cannot understand that, then perhaps the board itself is part of the governance problem."

Changing legislation and corporate accountability- what is impact for next generation?

PG: "This generation has more access to information than any generation before it and far more ways to distribute it. You can see that in the way people use Reddit, X and Google Reviews to expose bad conduct. Tolerance for misconduct is lower now, and that is good for society."

Evidencing your case

PG:" But I would still give one strong warning: do not start downloading gigabytes of company data and taking it home just because you think you are right.

There is a real difference between having the truth on your side and having the resources to fight a company in court. If you mishandle data, the company may sue you for theft before the underlying misconduct is ever tested."

PG: "The first step is to get legal advice before you do anything. In a highly regulated environment, unauthorized data transfers can end your career immediately.

In many cases, you do not need nearly as much data as you think. A safer approach is to record where the information sits so that a regulator, law-enforcement agency or the company itself can secure it properly once the matter is reported.

If you do need to preserve evidence yourself, your position is far stronger if you can show it was done solely to support a legitimate whistleblowing case and not for personal gain or to benefit a competitor.

Every case is different. The point is to avoid exposing misconduct by committing a separate breach on the way there."

C. Management Summary

In recent years, significant strides have been made in protecting whistleblowers, reflecting a growing recognition of their vital role in promoting transparency and accountability within organizations. Legislative frameworks, such as the EU Whistleblower Directive and various national laws, have been established to provide essential protection for individuals who expose wrongdoing. However, despite these advancements, substantial gaps remain in the legal landscape that still leave many whistleblowers vulnerable.

One of the most pressing issues is the persistent perception of whistleblowers as "problematic" rather than as heroes who uphold integrity and ethical standards. This stigmatization can lead to a culture of silence, where employees hesitate to report misconduct due to fears of retaliation or social ostracism. The white paper highlights that while organizations have made progress in implementing whistleblowing protections, the need for a cultural shift is paramount. Whistleblowers should be celebrated for their courage to speak up, and organizations must foster an environment that encourages open dialogue and values ethical behavior.

To effectively address these challenges, companies must take proactive steps to create psychological safety within their organizations. This includes incorporating cultural dimensions into their speak-up programs, ensuring that they resonate with diverse employee backgrounds. Furthermore, organizations must implement measurement systems to monitor potential retaliation against whistleblowers, fostering an environment where employees feel secure in voicing their concerns.

Regulators also play a crucial role in this ecosystem. They must improve existing laws to eliminate legal constraints that hinder reporting and ensure that whistleblower protections are robust and comprehensive. By doing so, they can help transform the narrative surrounding whistleblowing, shifting the perception from one of fear to one of empowerment.

Ultimately, the white paper advocates for a cultural shift that recognizes and rewards the integrity of whistleblowers, promoting an ethical workplace where speaking up is seen as a courageous act that contributes to the greater good.

D. Purpose & Focus of this Paper

D.1. Objective and Aims

As the regulatory landscape undergoes a paradigm shift toward radical transparency, the ENFCO Whistleblowing Framework serves as a blueprint for institutional integrity. This whitepaper is designed to bridge the gap between high-level legislative intent and the practical realities of compliance management.

The overarching aim of this whitepaper is to establish a Gold Standard for Whistleblowing Governance that transcends simple regulatory check-boxing. ENFCO seeks to provide a comprehensive roadmap that empowers organizations—particularly those within the regulated financial sector—to transform whistleblowing into a robust "early warning system" that protects the firm's reputation, its stakeholders, and the broader integrity of the global financial ecosystem.

To achieve this aim, the document focuses on four critical pillars designed for a multi-stakeholder audience:

- **For Compliance Professionals & MLROs**: To provide a granular, forensic guide to the Whistleblowing Lifecycle, ensuring that internal investigations are conducted with the highest levels of objectivity, evidence preservation, and psychological safety for the reporter.
- **For Regulated Entities & Boards**: To illustrate the Commercial and Strategic Value of a transparent culture, demonstrating how effective whistleblower protection acts as a primary tool for risk mitigation, fraud prevention, and long-term value preservation.
- **For Regulators & Governments**: To advocate for the Operationalization of International Standards (such as the EU Whistleblowing Directive), providing evidence of how private-sector excellence can support public-sector goals of crime prevention, anti-money laundering (AML), and market stability.
- **For External Stakeholders & Third Parties**: To define the Extended Perimeter of Protection, ensuring that contractors, vendors, and partners understand their vital role in the reporting ecosystem and the statutory safeguards that protect them from commercial or professional retaliation.

Whistleblowing legislation still contains many gaps, whistleblowers endure moral and financial stress when speaking up, so this ENFCO Whistleblowing Framework highlights the major gaps and makes recommendations for improvement (see section S).

Ultimately, the objective of this whitepaper is to advocate for a shift in perception: moving whistleblowing from the "Compliance Risk" category into the **"Corporate Resilience"** category. By aligning the interests of the whistleblower with the interests of the regulator and the organization, ENFCO provides a path toward an ethical future where integrity is the most valuable currency.

D.2. Intended Audience

This white paper is intended for a variety of different stakeholders, as shown in table 1.

Table 1: Summary Table of Stakeholder Interests

Stakeholder Group	Primary Interest in the Whitepaper
Front Line	Looking for tactical and forensic guidance
Regulators	Assurance that firms are meeting the “spirit” of the law
Investors	Proof of a healthy, non-toxic corporate culture
Third Parties	Confirmation of their legal safety when reporting

The Compliance & Operations Sphere (The "Front Line")

These are the primary users of the whitepaper, looking for tactical and forensic guidance.

- **Money Laundering Reporting Officers (MLROs) & Nominated Officers:** For guidance on SARs and financial crime intersections.
- **Chief Compliance Officers (CCOs) & Risk Managers:** For institutional risk frameworks.
- **Internal Auditors:** To understand how to audit the "Speak Up" culture.
- **HR Directors:** To align whistleblowing protocols with employment law and disciplinary procedures.

The Regulatory & Governance Sphere (The "Oversight")

These stakeholders look for alignment with public policy and legal mandates.

- **National Competent Authorities (NCAs):** (e.g., FCA in the UK, BaFin in Germany, GFSC in Gibraltar) interested in how private networks implement their directives.
- **European Supervisory Authorities (ESAs):** Including the EBA, ESMA, and EIOPA, focusing on cross-border financial stability.
- **Data Protection Authorities (DPAs):** Focused on the friction between whistleblowing and GDPR.
- **The European Commission:** Monitoring the transposition and effectiveness of the EU Whistleblowing Directive.

The Corporate & Investor Sphere (The "Strategic")

These stakeholders view whistleblowing through the lens of value and liability.

- **Boards of Directors & Audit Committees:** Seeking to understand their personal liability and "Duty of Care."
- **Institutional Investors & ESG Analysts:** Using whistleblowing health as a metric for "Social" and "Governance" scores.
- **Shareholders:** Interested in how whistleblowing prevents catastrophic fraud that devalues stock.

The External & Value-Chain Sphere (The "Perimeter")

These stakeholders are often the sources of the most critical disclosures.

- **Outsourced Service Providers:** (KYC firms, IT security, Cloud hosting) who need to know their reporting rights.

- **Legal Counsel & Law Firms:** Who advise both whistleblowers and corporations.
- **Professional Bodies & Networks:** Other compliance networks (like ACAMS or ICA) looking for collaborative standards.
- **Non-Governmental Organizations (NGOs):** (e.g., Transparency International) who advocate for whistleblower rights.

E. Structure of this Paper

This white paper is structured to guide the reader through the evolving role and strategic positioning of compliance within organizations. It is organized as follows:

- **Chapter F** Introduction
- **Chapter G** Global /regional whistleblowing regulations
- **Chapter H** Incentive structures for whistleblowers
- **Chapter I** Non-Disclosure Agreements (NDA)
- **Chapter J Expanding** the perimeter- third party and external stakeholders
- **Chapter K** Strategic Awareness: Educating & Empowering stakeholders
- **Chapter L** Psychological safety and reasons people do not speak up
- **Chapter M** What are some of the challenges for whistleblowers before, during and after they spoke up
- **Chapter N** Protecting the whistleblowers and anti-retaliation
- **Chapter O** Retaliation against Chief Compliance Officer
- **Chapter P** Challenges and opportunities recruiting whistleblowers?
- **Chapter Q** Principles of effective investigation
- **Chapter R** Specifics to the financial services sector
- **Chapter S** Recommendations
- **Chapter T** Interview with Pav Gill
- **Chapter U** Disclaimer
- **Chapter V** Acknowledgement

Together, these chapters provide a comprehensive view of the transformation of compliance from a legal safeguard to a strategic enabler of integrity and organizational resilience.

F. Introduction

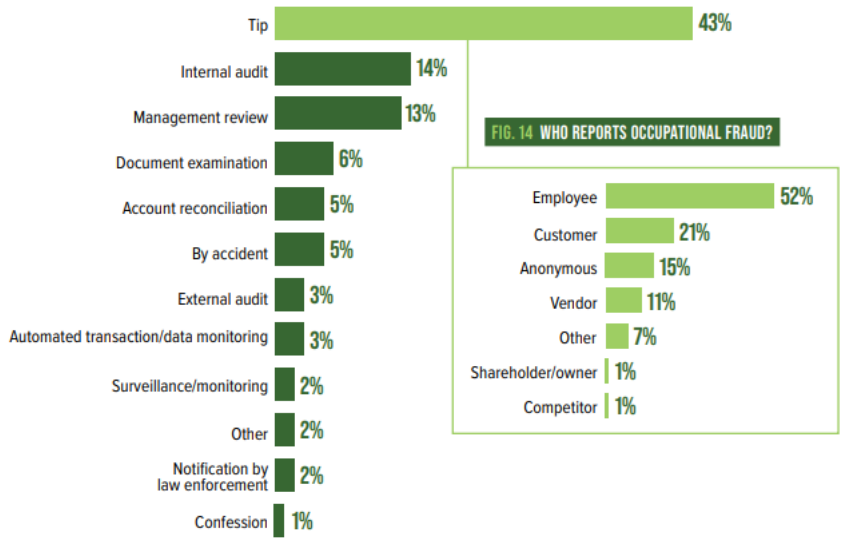
F.1. Introduction

Every year, companies and economies around the world lose **trillions of dollars** due to internal and external misconduct—from financial fraud to toxic workplace behavior. Occupational fraud schemes alone are estimated to cost organizations a collective **over $4.5 trillion** globally, while workplace violence, discrimination, and harassment generate **tens to hundreds of billions in losses** due to reduced productivity, absenteeism, legal costs, and reputational damage.

Workplace misconduct is not limited to financial wrongdoing. Issues such as harassment, discrimination, retaliation, and respect violations now account for most observed misconduct reports in many companies, dwarfing traditional fraud and accounting complaints.

Despite this staggering impact, a large proportion of misconduct never comes to light through ordinary controls, internal audits, or external inspections. Insider reporting by employees has repeatedly proven to be one of the most effective mechanisms for uncovering fraud, corruption, and systemic wrongdoing. In some global studies, whistleblower tips have been found to trigger detection in 43 % or more of occupational fraud cases, making them more effective than many traditional compliance tools combined.

Figure 1: How is occupational fraud detected?[1]



Yet the human cost of speaking up is far too high. Research[2] indicates that **85 % of whistleblowers report experiencing some form of retaliation** after reporting misconduct, and **30 % become unemployed** as a result. Many report significant stress, isolation, and lack of legal support following their disclosures.

According to Ethisphere ethical culture report[3] 93 % of employees said that they would report misconduct when they see it, however only 50% of employees reported it. This difference is called the “Speak-Up gap”.

Even when laws exist to protect them, **fear of retaliation remains one of the biggest barriers to reporting**, with most employees saying they would avoid speaking up because they don’t trust that their confidentiality will be respected or that they will be safe.

[1] 2026-report-to-the-nations.pdf
[2] Whistleblower Statistics: ZipDo Education Reports 2025
[3] 2271501_EthicalCultureReport-FirstFullDraftdue5-17_061324

These dynamics tell a stark story: organizations continue to under-utilize potentially their *most valuable* early-warning system, and many whistleblowers—rather than being seen as assets—are treated as liabilities.

F.2. What is whistleblowing?

The EU whistleblowing directive[4] does not define "whistleblowing" or "speaking up", it only refers to internal or external reporting of breaches of law.

Some define "speak up" as speaking up internally within an organization, and "whistleblowing" as speaking up externally, where information is communicated outside of the organization, for example to government agencies or the media.

In this working paper we will define Speaking Up and Whistleblowing as follows.

Speaking up means raising a concern, question, or idea about something that doesn't seem right or could be improved. Speaking Up is usually **internal** (to a manager, HR, or a colleague), covers a wide range of issues and is often focused on improvement and prevention e.g., raising concerns about unfair treatment, pointing out a safety risk at work.

Whistleblowing is the act of reporting **serious wrongdoing** that is illegal, unethical, or dangerous. It often involves **serious misconduct,** reporting might be done **internal or external** (regulators, authorities, media) and the reporters are often legally protected in many countries. Core categories include criminal offenses (e.g., money laundering, bribery, corruption, insider trading or fraud), breaches of legal obligations (e.g., regulatory non-compliance), exposing health and safety violations that could endanger lives or environmental damages. Whistleblowing usually involves a "Public Interest" element, where the matter transcends the individual and impacts the legal, ethical, or financial standing of the firm.

Table 2: The differences between Speaking Up and Whistleblowing are:

	SpeakUp	**Whistleblowing**
Scope	broad concerns / ideas	serious wrongdoing
Legal Protection	not always	often protected by law
Purpose	improve or prevent issues	stop harmful acts
Severity	low/moderate	high/critical

F.3. What is not whistleblowing?

The efficacy of a whistleblowing framework relies entirely on the quality of the disclosures it attracts. To maintain a functional system, a sharp distinction must be drawn between **protected whistleblowing**

[4] Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law

(reporting of wrongdoing that affects the organization or the public) and **personal grievances** (expressions of dissatisfaction regarding individual treatment).

To draw this line legally and operationally, we apply the **Reasonable Belief Test**. For a disclosure to qualify as whistleblowing:

1. **Subjective Belief:** The reporter must genuinely believe the information is true.
2. **Objective Reasonableness:** A neutral third party, given the same information, would agree that the information points to a breach of law or regulation.

A critical challenge for the Compliance (and/or MLRO) function is the "weaponization" of reporting channels. Mechanisms intended to surface systemic risk are often misappropriated by disgruntled stakeholders—such as terminated employees or unsuccessful business partners—as a tool for leverage or retaliation.

To mitigate this, we define the following as **out-of-scope** for the whistleblowing policy:

Category	**Description**	**Proper Channel**
Personal Grievances	Issues concerning an individual's employment contract, promotion denials, or interpersonal conflicts.	Human Resources / Internal Grievance Policy
Commercial Disputes	Disagreements over contract terminations, pricing, or lost bids by business partners.	Legal / Procurement Dispute Resolution
Malicious Reporting	Reports made with the primary intent of causing reputational harm, knowing the information is false.	Disciplinary Action / Legal Recourse
Vexatious Claims	Repeatedly filing the same unsubstantiated claim to disrupt company operations.	General Management / Legal

F.4. Importance of whistleblowers for corporate governance, compliance and ethics

Whistleblowers help companies in numerous ways:

1) Encouraging employees to speak up when they have an ethic and compliance question or concern creates a significant advantage for your organization. It means you have an early warning system in place that allows you to address potential issues before they escalate – and better protect your organization from reputational, financial and legal risk.

2) Whistleblowing reinforces the ethics and compliance program and strengthens a culture of accountability.
3) creates a positive ripple effect in the organization. When other employees see that whistleblowing and transparency is encouraged and wrongdoers are punished, they are more likely to speak up

G. Global and Regional regulations

G.1. USA

The U.S. does not have one single whistleblower law, but whistleblowing protections are largely industry-specific, meaning the rules, reporting channels, and protections depend on what sector you work in and what kind of misconduct is involved. This means that employees can report misconduct to regulators even if they signed an NDA.

Employees of publicly traded companies are typically protected under Sarbanes-Oxley Act and Dodd-Frank Act for whistleblowing reporting on accounting fraud, securities fraud, internal control violations and/or misleading investors.

Employees and/or (sub) contractors of government contracting or defense companies provide whistleblower protections under the False Claims Act for reporting fraud against the US government such as defense contracting fraud, overbilling, false invoices or defective products.

In the pharma and healthcare sector, whistleblower protections are provided under the False Claims Act for reporting kickbacks, Medicare /Medicaid fraud, false clinical trial data or unsafe medical practices.

In the financial services industry, reporting violations of banking regulations or financial harm to consumers is protected under the Federal Deposit Insurance Act (FDIA) and Dodd–Frank Act.

Reporting environmental violations, reporting public health risks or reporting nuclear safety risks are protected under various laws (e.g. Clean Air Act, Clean Water Act, Toxic Substances Control Act).

Whistleblower Protection Act (WPA) and Whistleblower Protection Enhancement Act (WPEA) protect whistleblowers that report Waste, fraud, and mismanagement and violations of law by federal agencies.

Whereas whistleblower protection laws exist by industry and provide protection depending on channels used and kind of misconduct reported, this also means that reporting “general unethical behavior” that is not illegal is usually not protected. It is also worth noting that some laws protect whistleblowing to regulators (=external reporting) but not employees reporting internal complaints.

In the private sector, employees in non-profit organizations, small private businesses with no government contracts or employees in retail or hospitality industry often do have weak or nonexistent whistleblower protection. With a few exceptions many federal laws protect only employees, not contractors.

G.2. EU Whistleblower Directive

Whistleblowing protection in the EU is much broader than in United States and applies to the reporting of breaches of EU law (e.g. public procurement, money laundering, terrorist financing, consumer protection, environmental protection, public health, competition and state aid rules, fraud/corruption, transportation safety, data protection and privacy law, financial services, banking and insurance law). The EU Directive does not only cover employees in public and private sector but also part-time, temporary, and fixed-term workers, agency workers, trainees and interns, volunteers, self-employed people, former employees but also shareholders and members of company boards

Whistleblowing is not protected under the EU Directive if it relates to purely ethical concerns, workplace grievances (harassment, pay disputes), unless linked to EU-law breaches, policy disagreements and lawful but unpopular conduct. Also, if whistleblowing is done publicly without first using internal/external channels, unless there is imminent danger or risk of retaliation, then protection might be lost.

The Directive requires both internal (to the employer) and external (to competent authorities) reporting channels. Some Member States went further by establishing independent authorities to receive reports (e.g., Spain). Others rely more on centralized or pre-existing institutions.

The Netherlands has a recognized independent body known as the *"Huis voor klokkenluiders*" (House for Whistleblowers). It serves as a specialist authority providing advice, support, and an external reporting outlet for whistleblowers, and is a key part of the whistleblowing framework following the Directive's implementation.

Spain has created a fully independent authority *Autoridad Independiente de Protección del Informante* tasked with receiving external reports of wrongdoing, overseeing compliance with national whistleblowing law (Law2/2023), protecting whistleblowers, and managing external reporting channels. It operates with functional autonomy from other branches of government.

Ireland's national whistleblower regime under the Protected Disclosures Act predates the EU Directive and includes statutory frameworks for external reporting. While not always described as a new independent authority, Ireland designates competent authorities across sectors and has statutory safeguards for external reporting mechanisms that act independently for whistleblower matters.

Many EU countries designate competent authorities that, while not always created as new standalone bodies, serve as external reporting authorities under transposition laws. These authorities may be existing regulators or agencies but effectively function independently of employers to receive and handle whistleblower reports, often with statutory guarantees of confidentiality and impartiality. Examples include:

- Belgium — Federal Ombudsman (designated competent authority in Belgian implementation).
- France — Défenseur des droits (independent rights defender office) acts as whistleblower competent authority.
- Germany — Federal Office of Justice and other sectoral authorities handle external reports.
- Italy — National Anti-Corruption Authority receives external reports.
- Romania — National Integrity Agency serves as authority for external whistleblower reporting.
- Czech Republic — Ministry of Justice acts as competent authority

In several EU Member States, anonymous reports can be submitted, but employers or authorities are not legally obliged to investigate or follow up: Czech Republic, Denmark, Estonia, Finland, France, Hungary, Ireland, Italy, Spain and Sweden.

G.3. UK Law

Whistleblowers law (Public Interest Disclosure Act) protects workers who make a **"protected disclosure"** about wrongdoing in the **public interest**.

A disclosure is protected if the worker reasonably believes it shows one or more of the following: a criminal offence, breach of a legal obligation, miscarriage of justice, danger to health and safety, environmental damage or deliberate concealment of any of the above. The disclosure must be made **in public interest** (not just a personal grievance).

PIDA protects a narrower group than the EU Directive. Employees, Agency workers, some contractors and freelancers, trainees, national health service workers and doctors are protected against retaliation, but non-executive directors, self-employed individuals, shareholders, volunteers and job applicants are not covered.

Except for the regulated sector, there is no obligation for private employers to set up a whistleblowing system. Anonymous reporting in the UK is allowed, however there is no formal obligation for private employers to investigate the allegations.

G.3.1. Legal Guardrails: Preventing Bad-Faith Reporting in the UK

In the United Kingdom, the legal framework is specifically designed to protect "workers" who speak up, but it includes stringent criteria to ensure the system is not weaponized for personal gain or used to settle workplace grievances.

The following "guardrails" are essential for any organization to understand when drafting their internal policies.

G.3.1.1 The “Public Interest” Test

Following the **Enterprise and Regulatory Reform Act 2013**, a whistleblower must show they "reasonably believe" the disclosure is made **in public interest**.

- **The Guardrail:** This prevents individuals from gaining legal protection for reporting personal or private grievances (e.g., a disagreement about an individual's own employment contract).
- **Corporate Application:** Policies should clearly distinguish between a "Personal Grievance" (handled by HR) and a "Protected Disclosure" (handled by the Whistleblowing Officer).

G.3.1.2 The “Reasonable Belief” Standard

UK law does not require a whistleblower to be *correct* about the wrongdoing, but they must have a **reasonable belief** that the information tends to show malpractice has occurred, is occurring, or is likely to occur.

- **The Guardrail:** Speculation, office gossip, or baseless rumors do not meet this threshold. If a report is found to be based on zero evidence or is intentionally fabricated, the individual loses all statutory protection against dismissal or detriment.

G.3.1.3 The “Good Faith” Adjustment (section 123 of ERA)

While "good faith" is no longer a requirement for a disclosure to be *protected* (to ensure even disgruntled employees can report genuine fraud), it remains a powerful financial deterrent.

- **The Guardrail:** If an Employment Tribunal finds that a disclosure was made in **bad faith** (e.g., out of malice or for personal leverage), the court has the power to reduce any compensation awarded to the whistleblower by up to **25%**.
- **Impact:** This discourages "tactical whistleblowing," where an employee might report a minor issue solely to avoid a pending disciplinary action.

G.3.1.4 Restrictions on “Gagging Clauses”

Under **Section 43J of PIDA**, any clause in a settlement or employment agreement that purports to prevent a worker from making a protected disclosure is void.

- **The Guardrail:** While this sounds like protection for the whistleblower, it also acts as a guardrail for the system's integrity. It ensures that "hush money" cannot be used to hide systemic failures, keeping the focus on the **truth of the information** rather than a financial transaction.

G.3.1.5 Vicarious Liability and "reasonable steps"

UK law (since 2013) makes employers liable for any "detriment" (bullying or harassment) inflicted on a whistleblower by their colleagues.

- **The Guardrail:** However, an employer has a legal defense if they can prove they took **all reasonable steps** to prevent such treatment.
- **Best Practice:** This incentivizes companies to provide training and clear reporting paths, which naturally filters out low-quality or malicious reports by establishing a formal, evidenced process.

G.3.1.6 Summary of UK Safeguards

Table 3: Summary of UK safeguards

Guardrail	**Legal Mechanism**	**Protection Against...**
Public Interest Test	PIDA Section 43B(1)	Use of whistleblowing for private/personal grievances.
25% Award Reduction	Section 123(6A) ERA	Malicious reporting or "bad faith" motivations.
Reasonable Belief	Statutory Requirement	Baseless rumours or intentionally false accusations.
Internal Procedures	Case Law (e.g., *Chesterton*)	Bypassing the company to go straight to the media for profit.

G.4. Switzerland

Switzerland does not have a general whistleblower protection statute comparable to the EU Whistleblower Directive, or the UK's Public Interest Disclosure Act (PIDA).

Whistleblowing in Switzerland is mainly governed by Swiss Code of Obligations (CO) and Article 321a CO: that says that employees have a duty of loyalty to the employer. Employees are expected to protect the employer's interests, including confidentiality.

Swiss courts follow a step-by-step doctrine (case law, not statute) for private sector employees whereby whistleblowers are expected to report first internally to the employer. If the employer does not take any action, then reporting can be done to the authorities. Reporting to the media should happen only if internal and official external channels have failed and there is serious wrongdoing by the company and there is urgent public interest

Public sector employees are slightly better protected. Federal public servants are protected when reporting to supervisors, federal audit office criminal offenses, corruption of serious irregularities.

Job applicants, former employees, volunteers, interns, contractors, freelancers, facilitators (colleagues, lawyers) and shareholders that are explicitly protected in the EU Directive are all not protected under Swiss law.

Anonymous reporting is allowed in practice, but employers are not required to investigate anonymous reports.

NDAs and confidentiality clauses are strictly enforced with no broad statutory exception for whistleblowing.

G.5. The Legal Charter: Protections, Rights, and Responsibilities

This section synthesizes the global standards set by the **EU Whistleblowing Directive (2019/1937)**, the **US Sarbanes-Oxley (SOX)** and **Dodd-Frank Acts**, and the **UK Public Interest Disclosure Act (PIDA)**. For an MLRO, this represents the "Legal Charter" that governs the relationship between the firm and the reporter.

In the eyes of international regulators, the whistleblower is a "protected participant" in the justice system. To maintain this status, there is a reciprocal relationship: the law provides robust shields, but the whistleblower must adhere to specific procedural standards.

G.5.1. Statutory Protections ("The Shields")

International legislation focuses on shielding the whistleblower from any "detriment" resulting from their disclosure.

- **Absolute Prohibition of Retaliation:** This is the cornerstone of all global regulations. Protection extends beyond dismissal to include demotion, salary reduction, transfer of duties, or any form of harassment.
- **The "Reverse Burden of Proof":** In many jurisdictions (notably the EU), if a whistleblower suffers a detriment, the *employer* must prove in court that the action was entirely unrelated to whistleblowing.
- **Interim Relief:** Rights to seek a court order to stay a dismissal or suspension while a whistleblowing claim is being litigated, ensuring the individual is not financially "starved out" during the process.

- **Immunity from Liability:** Whistleblowers are protected from civil or criminal liability for breaching confidentiality, data protection, or trade secret laws, provided the disclosure was necessary to reveal the misconduct.

G.5.2. Rights of the Whistleblower (“The Entitlements”)

A whistleblower is entitled to expect the following from the organization and the authorities:

- **Right to Anonymity/Confidentiality:** The right to have their identity protected at all stages. Disclosure of the identity should only occur with consent or under extreme legal mandate (e.g., in a criminal trial).
- **Right to Feedback:** Under the EU Directive, whistleblowers have the right to be acknowledged within 7 days and to receive feedback on the progress/outcome of the investigation within 3 months.
- **Right to External Reporting:** If internal channels are compromised or ignored, the individual has the right to report directly to a competent regulatory authority (the "Regulatory Bypass").
- **Right to Support Measures:** Access to free legal advice and psychological support, often facilitated through state-appointed bodies.

G.5.3. Responsibilities of the Whistleblower (“The Obligations”)

Protection is not absolute; it is contingent upon the whistleblower acting with integrity.

- **The "Reasonable Grounds" Test:** The reporter must have had a reasonable belief that the information disclosed was true at the time of reporting. Protection is **not** granted to those who knowingly report false or misleading information.
- **Duty of Confidentiality Regarding the Investigation:** While the reporter has a right to report, they have a responsibility not to compromise the investigation by leaking details to the press or unauthorized parties while the process is ongoing.
- **Compliance with Internal Procedures:** Whistleblowers are generally encouraged (though not always strictly required) to use established internal channels first, provided those channels are safe and functional.
- **Proportionality in Data Gathering:** While they may access data to prove a breach, they have a responsibility not to engage in "industrial espionage" or the mass theft of unrelated proprietary information.

G.5.4. Summary Matrix for Global Compliance

Feature	Whistleblower Entitlement	Whistleblower Obligation
Integrity	Right to be taken seriously.	Must believe the report is true (Good Faith).
Privacy	Identity must be shielded.	Must keep the investigation confidential.
Employment	Protection from demotion/firing.	Must continue to perform duties professionally.
Evidence	Immunity for necessary data access.	Must not steal unrelated trade secrets.

H. Incentive structures for whistleblowers

The US and Europe have different legal systems, different enforcement philosophy and different values and attitudes on rewarding whistleblowers.

H.1. Regulatory models

Under the False Claim Act, employees, suppliers, contractors or other outsiders with original information of fraud against the US government can get rewards of 15-30% of money recovered by the government.

Under the SEC whistleblower program, employees, contractors, third parties that provide evidence of securities law violations (insider trading, accounting fraud, market manipulation, false disclosures to investors etc.) can get rewards of 10-30% of sanctions collected over $1 million.

Like SEC Whistleblowing, the CTFC Whistleblowing program provides awards of 10-30% of sanctions collected over $1 million for those providing evidence of irregularities in commodities and derivative markets (e.g. market manipulation, fraud is futures or swaps)

IRS Whistleblowing program provides awards of 15-30% of collected taxes and penalties to anyone who provides credible information regarding corporate tax fraud, hidden income schemes or tax evasion.

Outside the United States, there are virtually no or very little incentives or rewards for whistleblowing. In most European countries, UK and Switzerland, whistleblowing is treated as a public duty, not a paid activity.

H.1.1. Pros

Incentives and rewards can be justified when violations are hard to detect, government recovery is high, enforcement relies on insiders and evidence is internal.

Whistleblowers often face job loss, legal costs, mental health stress, long-term career harm. Financial rewards are created to make whistleblowing economically feasible and compensate for (irreversible) personal damage.

Incentives create a strong deterrence effect for wrongdoing. Incentives for whistleblowers encourage better compliance programs as companies know that insiders have strong incentives to report.

Reward systems typically require original, credible, and well-documented information, and cooperation with regulatory investigations which incentivize whistleblowers to provide strong evidence, filters out vague complaints and often leads to the recovery of billions which is positive for taxpayers.

H.1.2. Cons

Reporting wrongdoing is seen as a civic duty, and paying incentives to whistleblowers is considered morally questionable and encouraging disloyalty.

Giving incentives to whistleblowers might discourage employees to report issues internally and/or incentivize employees to wait for misconduct to continue /grow to take advantage of financial incentives.

In Europe there are also ethical questions around paying incentives to whistleblowers for misconduct they might have participated in. Doing so is probably unjust to victims of misconduct.

Finally, incentivizing whistleblowing reporting might lead to increased reporting of weak allegations, tactical reporting in employment disputes or personal vendettas.

The EU prioritizes « Internal reporting first", organizational responsibility and prevention over punishment. Rewarding whistleblowers is seen as encouraging "external escalation first" and weakening internal governance.

EU Member States have very different legal traditions, labor protections and cultural attitudes so introducing financial rewards to whistleblowers would complicate harmonization in the EU, would create cross-border disputes and would be politically divisive. EU policymakers also feared that whistleblowing would shield against dismissal.

H.2. Should organizations provide financial incentives for speaking up?

H.2.1. The Global Divergence

The use of financial incentives in whistleblowing frameworks should be assessed primarily through the lens of effectiveness in detecting and deterring misconduct, rather than cultural or philosophical preferences. Whistleblowing is one of the most effective detection mechanisms for fraud and misconduct, yet reporting remains systematically underutilized due to high personal and economic costs borne by whistleblowers.

H.2.2. The Philosophical Divide

Regulatory approaches can broadly be categorized into two models, but this distinction should be understood as a difference in policy design choices rather than normative superiority.

- The United States (Incentive-Based model)
    - The US framework incorporates financial incentives as a core enforcement tool. Programs such as SEC Whistleblower Program and the False Claim Act provide rewards (typically 10-30% of recovered sanctions) only where original, credible information leads to successful enforcement action.
    - Empirical evidence shows that such systems:
        - Significantly reduce financial reporting fraud (Wiedman and Zhu)
        - Improve corporate compliance and internal controls (Wiedman and Zhu)
        - Enhance detection and deterrence, particularly in environments where misconduct is difficult to uncover (Spagnolo, Giancarlo & Theo Nyreröd. "A Fresh Look at Whistleblower Rewards." *Journal of Governance and Regulation* , vol. 10, no. 4 (Special Issue), 2021.

- **European and the UK (Protection-based model)**

  European frameworks emphasize protection from retaliation rather than financial incentives. While this approach strengthens legal safeguards, it does not address the economic disincentive to report wrongdoing, nor the documented "speak-up gap" between willingness to report and actual reporting behavior.

  Academic literature increasingly highlights that protection alone is insufficient to maximize reporting effectiveness, particularly in high-risk cases involving corruption or financial misconduct (Spagnolo and Nyrerod).

H.2.3. Mitigating the risks of financial incentives

Concerns regarding financial incentives primarily relate to potential misuse, including false or opportunistic reporting. However, empirical and legal analysis shows that such risks can be effectively mitigated through program design.[5] To address these concerns, the best global practices have evolved to include specific "guardrails":

1. **Thresholds of Originality and Materiality:** To qualify for a reward in systems that offer them, the information must be "original" and not already known to the regulator or the public and it must materially contribute to the outcome.
2. **The Good Faith Requirement:** Reporting must be based on a reasonable belief that the information is true. In many jurisdictions, rewards are forfeited, and legal protections are removed if the report is found to be intentionally malicious.
3. **The "Dirty Hands" Exclusion:** Individuals who planned or initiated the misconduct are typically barred from receiving financial rewards, ensuring that the system is not exploited by the perpetrators themselves.

H.2.4. Best Practices: a “remedial” approach for Europe

For European jurisdictions, the introduction of financial incentives should not replace protection-based systems but complement them to enhance effectiveness. Financial incentives should be framed as compensation for risk exposure and contribution to prevention of loss, rather than as profit.

- Compensation and reward mechanism may co-exist
- Compensation for losses (legal costs, loss of income)
- Discretionary rewards linked to outcomes
- Interim Relief: providing financial support during the investigation or litigation process prevents the “financial strangulation” of the reporter, which is a common tactic used by retaliating parties.
- Outcome-based reward design
    - Where financial incentives are used, they should be linked to seriousness of misconduct, reputation or public interest impact or successful outcomes.

[5] Buccirossi, Paolo & Immordino, Giovanni & Spagnolo, Giancarlo, 2017. "Whistleblower Rewards, False Reports, and Corporate Fraud," SITE Working Paper Series 42, Stockholm School of Economics, Stockholm Institute of Transition Economics, revised 29 Aug 2017.

H.2.5. Summary of Recommendations

Recommendation	Objective
Prioritize Protection	Focus on robust anti-retaliation measures before considering financial incentives.
Promote effectiveness alongside integrity	Financial incentives are recognized as a legitimate tool to enhance detection, while maintaining strong internal reporting systems.
Discretionary and proportionate rewards	Financial incentives remain discretionary, proportionate, and linked to measurable benefit.
Strict eligibility and verification criteria:	Rewards are granted only where: information is original and credible, reporting materially contributes to outcome, misconduct is substantiated.

A valid alternative for European Companies would be as well to consider introducing non-financial rewards and recognition programs.

H.2.6. Non-financial incentives and recognition programs

There are several actions companies can take and incentives they can introduce to promote a “speak-up” culture and reinforcing integrity:

1) The Compliance or Ethics & Compliance team can provide “thank you letters” to whistleblowers
2) Leadership can provide (confidential) recognition to whistleblowers
3) Other forms of appreciation
4) The company can provide psychological support or confidential legal advice to overcome stressful situations when speaking up,
5) Managers are evaluated on speak-up responsiveness and psychological safety
6) Teams are rewarded on early issue escalation and transparency

H.2.7. When to consider incentives

Incentives should not be designed to create speculative or opportunistic reporting, but to correct the imbalance between high personal risk and the benefit inherent in whistleblowing. Across the EU, UK, Switzerland, and most non-US jurisdictions cash rewards tied to allegations or outcomes shouldn’t be the main driver for reporting.

To overcome a fear of speaking up (e.g. low hotline usage despite high risk, repeated survey results showing fear of retaliation or cultural silence in high-risk regions), a company could consider primarily introducing protective incentives such as recognition, legal support, explicit career guarantees that there will not be negative consequences for speaking up, independent oversight of HR decisions etc.

Companies should retain discretion to provide financial incentives, but such discretion should be exercised within a **clear, evidence-based framework recognizing the proven benefits of incentives for detection and deterrence** (Spagnolo and Nyreröd; Wiedman). When doing so, they should consider the various advantages and disadvantages and should have clear policies and procedures in place, outlining in which cases and under which circumstances such incentives will be awarded or not.

H.2.8. When not to consider incentives

When the organization or company already has a strong speak-up culture evidenced by healthy reporting levels, high trust in investigations and low retaliation incidents, no additional incentives or rewards may be required, and the company might adapt its policies and procedures to reflect that new and more mature company culture.

During periods of restructurings, layoffs, performance management cycles incentives can be misused (“weaponized”) for job protection, so companies should be aware of this.

Incentives should not be used to compensate for weak management or lack of accountability.

H.3. Aligning whistleblowing and incentives with organizational culture

High-trust organizations frame whistleblowing as protecting colleagues, protecting customers, protecting the organization and as part of professional responsibility.

Different organizational cultures require a different emphasis of Speak Up e.g.:

- In hierarchical cultures, it is important to emphasize strong anti-retaliation elements and independence of reporting.
- In global organizations, multilingual and culturally sensitive reporting channels should be promoted
- In high-risk environments, formal reporting channels and anonymity should be promoted.

Even though organizations should have a global commitment to integrity (global values), communication and messaging around Speak-up must be adapted locally. What works in the USA might not work in the Middle East, Asia, Central Europe etc.

Employees speak up when they believe reports will be taken seriously, investigations are fair, outcomes are proportionate and retaliation will be addressed. Therefore, as part of organizational culture the process for reporting issues and investigations should be explained transparently, consequences for misconduct should be consistently applied (regardless of seniority in the organization).

H.4. Best Practice Recommendation

A company's global whistleblowing policy should consistently state that speak-up is encouraged, retaliation is prohibited, reports can be made anonymously (where lawful), confidentiality and good-faith reporting is protected even if unsubstantiated.

In USA a company must explicitly acknowledge the legal right of whistleblowers to report to regulators, and a company should not discourage or penalize whistleblowers for external reporting. Likewise, a company cannot require that internal reporting should happen first.

Within Europe, companies should emphasize and promote internal reporting as the preferred route and should consider preventing bad faith reporting as seen in the UK.

Companies and regulators should explicitly recognize that financial incentives for whistleblowers are a legitimate and evidence-based tool to enhance detection, deterrence and effectiveness. While remaining discretionary, such incentives should be:

- Linked to the outcomes
- Proportionate to public and/or company benefit
- Subject to strict eligibility criteria
- Integrated with strong anti-retaliation protections

A whistleblowing framework that relies solely on protection mechanisms is structurally incomplete, whereas a framework combining protection with targeted financial incentives is significantly more effective in achieving early detection of serious wrongdoing.

I. Non-Disclosure Agreement (NDA)

A non-disclosure agreement (NDA) is a legal contract in which one or more parties agree not to share certain confidential information with others. Typically, an NDA set clear rules about what information is confidential (e.g., trade secrets, intellectual property, client data etc.), how the confidential data can (not) be used, how long confidentiality lasts and consequences for breaking the NDA.

For employers, NDAs help prevent harm to the business as they protect sensitive information, reduce legal and financial risk and provide clear legal remedies if confidential information is leaked.

I.1. NDA versus whistleblowing

In many countries, NDAs cannot legally prevent whistleblowing, even if the agreement appears to prohibit disclosure. Many jurisdictions have whistleblower protection laws that allow confidential information to be disclosed for the purpose of reporting misconduct. If someone reports wrongdoing to regulators, law enforcement, or protected authorities, NDAs generally cannot be enforced against them.

I.2. Legal and ethical risks of overbroad NDAs

Sometimes NDAs are used to **intimidate or silence employees**, even though they would not hold up legally if challenged.

It is crucial for businesses to carefully draft NDAs to avoid these risks and ensure that they provide ad equate protection or sensitive information while allowing employees the freedom to report misconduct when necessary.

NDAs that restrict employees' ability to report misconduct to government agencies can be illegal and overly broad NDAs can be deemed unenforceable by courts due to vague definitions, unreasonable duration and broad scope.

I.3. Ensuring NDAs do not restrict legitimate whistleblowing

This is a critical area of compliance, as the "chilling effect" of overly broad NDAs has recently come under intense scrutiny from both regulators and the public.

In English, the terminology often refers to "gagging clauses" and the legal protections afforded by the Public Interest Disclosure Act 1998 (PIDA). This is a critical area of compliance, as the "chilling effect" of overly broad NDAs has recently come under intense scrutiny from both regulators and the public.

In UK English, the terminology often refers to "gagging clauses" and the legal protections afforded by the **Public Interest Disclosure Act 1998 (PIDA)**.

While Non-Disclosure Agreements (NDAs) and confidentiality clauses are legitimate tools for protecting proprietary information and trade secrets, they must never be used as a "gagging order" to prevent the reporting of wrongdoing. Within the European and UK regulatory landscape, any contractual term that purports to prevent an individual from making a protected disclosure is generally void and unenforceable.

I.3.1. The Risk of Restrictive Language

The primary danger is not always an explicit ban on whistleblowing, but rather the use of **broad, exclusionary language** that creates a "chilling effect." If an employee fears that speaking to a regulator will result in a breach of contract or financial penalty, the internal reporting system has failed.

I.3.2. Language to avoid

The following wording should be avoided:

- **"For any reason whatsoever":** Clauses that prohibit sharing information with "any third party for any reason" without explicitly exempting regulators.
- **Prior Notification Requirements:** Clauses requiring the individual to notify the legal department before speaking to a government body or regulator.
- **Threats of Forfeiture:** Terms suggest that "all severance benefits will be forfeited" if any information regarding the company's operations is shared.
- **Vague Definitions of "Confidential Information":** Overly wide definitions that could be interpreted to include evidence of criminal activity, breaches of legal obligations, or miscarriages of justice.

I.3.3. Implementing "Safe Harbour" Provisions

To ensure compliance and foster a culture of transparency, NDAs should include explicit "Safe Harbour" clauses. These clauses clarify that the agreement does not override the individual's statutory rights.

I.3.3.1 Best Practice Clause Examples:

1. **The Overriding Provision:** "Nothing in this Agreement shall prevent, or is intended to prevent, the Employee from making a 'protected disclosure' as defined by the Public Interest Disclosure Act 1998, or from reporting a suspected relevant offence to any competent authority or regulator."
2. **The Non-Interference Clause:**
   "Nothing in this Agreement shall preclude the Participant from communicating directly with, or providing information to, a government body or any other entity permitted by law regarding a possible violation of law or regulation, without notice to the Company."
3. **The Carve-Out for Legal Proceedings:**
   "Confidentiality obligations herein shall not apply where disclosure is required by law, court order, or requested by a law enforcement agency or the Financial Conduct Authority (FCA)."

I.3.4. Recommendations for Compliance Officers

- **Standardize Templates:** Ensure that all settlement agreements and employment contracts are reviewed to remove legacy "gagging" language.
- **Explicit Affirmation:** In exit interviews where an NDA is signed, verbally affirm that the agreement does not prevent the individual from speaking to the authorities regarding misconduct.
- **The "Clear English" Test:** Ensure the carve-outs are not buried in fine print. A whistleblower should not need a law degree to understand that they are still permitted to report fraud or safety violations.

Note: In the UK, the Solicitors Regulation Authority (SRA) and the Financial Conduct Authority (FCA) have issued specific warnings against the misuse of NDAs. Failure to include these carve-outs may not only render the NDA unenforceable but could also lead to regulatory sanctions against the firm.

I.3.5. Navigating the EU Whistleblowing Directive (2019/1937)

For ENFCO members operating across Member States, it is vital to align the NDA language with **Directive (EU) 2019/1937**. Article 24 explicitly prohibits any contractual or employment-related waiver of the rights and remedies provided for in the Directive.

- **The "Anti-Waiver" Principle:** Any clause that attempts to limit a whistleblower's right to report (internally or externally) is legally void.
- **Breadth of Protection:** Unlike some legacy UK contracts that focused only on "criminal acts," the EU Directive covers a vast range of breaches, including public procurement, financial services, and environmental protection. NDAs must be drafted to reflect this wide net.

I.3.6. The Hazard of "Claw back" and Forfeiture clauses

A particularly aggressive trend in employment litigation involves "claw back" clauses—provisions that require an employee to repay severance or bonuses if they "disparage" the company or breach confidentiality.

When applied to whistleblowing, these are not only unethical but often legally indefensible.

Why claw backs risk regulatory Action?

1. **Financial Coercion:** If a disclosure is protected by law, any attempt to recover funds based on that disclosure is likely to be viewed by courts as an unlawful detriment or "victimization."
2. **Obstruction of Justice:** In some jurisdictions, including the UK, attempting to financially penalize a witness for communicating with a regulator (like the FCA or PRA) can be treated as a contempt of court or a regulatory breach.

Best Practice for drafting "Repayment" terms:

To ensure these clauses do not inadvertently catch legitimate whistleblowers, include a **"non-derogation"** sentence immediately following any claw back provision:

> *"For the avoidance of doubt, the repayment obligations set out in this Clause [X] shall not be triggered by, nor apply to, any disclosure made by the Individual that constitutes a 'protected disclosure' under applicable whistleblowing laws, nor shall they apply to any communication with a competent regulatory authority."*

I.3.7. Recommended "Safe Harbour" Checklist

When auditing your organization's templates, ensure every NDA or Settlement Agreement passes the following "Safe Harbour" test:

Feature	**Requirement**
Explicit Carve-out	Does the text explicitly mention that the signatory is *not* prohibited from reporting to a regulator?
Statutory Reference	Does it refer to the relevant legislation (e.g., PIDA 1998 or the EU Whistleblowing Directive)?

No "Prior Consent"	Have you removed any requirement for the individual to seek permission before speaking to an authority?
Non-Disparagement	Is the "non-disparagement" clause qualified so it doesn't silence truthful reports of misconduct?
Financial Neutrality	Is it clear that no financial penalty (claw back) will result from a protected disclosure?

I.3.8. Case Studies and regulatory warnings

The shift in the regulatory landscape has moved from "disliking" restrictive NDAs to actively punishing firms that use them. Compliance Officers should be aware of the following developments to brief their Boards effectively.

I.3.8.1 Case Study: the “Integrity” Breach (FCA& Non-Financial Misconduct)

In recent enforcement actions (notably the 2025/2026 findings regarding **Crispin Odey** and subsequent "Dear CEO" letters), the UK’s **Financial Conduct Authority (FCA)** has clarified that mishandling reports of non-financial misconduct—such as sexual harassment or bullying—is a direct breach of the duty to act with integrity.

- **The Lesson:** If an NDA is used to settle a harassment claim but fails to explicitly state that the victim can still report the conduct to the regulator, the firm itself may be investigated for "lacking the necessary culture" and "obstructing the regulator’s functions."
- **The Penalty:** The FCA has shown a willingness to double fines to achieve "deterrence" in cases where firms have prioritized their reputation over their regulatory reporting obligations.

I.3.8.2 The Victims and Prisoners Act 2024 (Uk)

Effective **1 October 2025**, this Act introduces a statutory bar on NDAs that prevent victims of crime from disclosing information to:

- Law enforcement or regulators.
- Qualified lawyers or regulated professionals.
- Support services and close family members.

Warning for Compliance: Any NDA signed after this date that lacks these "permitted disclosure" carve-outs is partially void. Relying on "standard templates" created before late 2025 is a significant compliance risk.

I.3.8.3 Summary: A warning to the Board

Compliance Officers should present the following "Bottom Line" to the Board of Directors (or similar depending on the jurisdiction they are active in):

> **"The Board must understand that an NDA is not a shield against transparency. In the eyes of the FCA, PRA, and EU regulators, any attempt to buy a whistleblower's silence is an admission of poor governance."**

Key Takeaways for the Board:

- **Personal Liability:** Under the **Senior Managers and Certification Regime (SM&CR)**, the individual responsible for the firm's whistleblowing policy can be held personally accountable if NDAs are found to be systemically restrictive.
- **Reputational Backfire:** "Gagging clauses" often generate more negative PR than the original issue they sought to hide. Courts and tribunals are increasingly critical of "oppressive" settlement terms.
- **The Ethics Audit:** The Board should mandate an annual audit of all settlement agreements to ensure they meet the **"Clear English"** and **"Safe Harbour"** standards outlined in this paper.

I.4. Preventing weaponization of NDAs

In many cases, companies use NDAs not to protect confidential information but to bury allegations of misconduct. This practice effectively shields wrongdoers, enabling them to continue their harmful behavior with impunity. The victims, burdened by the weight of silence, are left to grapple with the trauma of their experiences while their abusers walk free, shielded by legal agreements meant to suppress the truth.

It is important to understand that signing an NDA takes a toll on people's wellbeing as the agreement typically forbids employees from confiding in friends or family about what they have experienced – and about the consequences. It prevents people from seeking counselling or medical help, unless a practitioner can be found who is also willing to sign an NDA: not an easy task.

It is crucial for all individuals to know their rights when presented with an NDA and to seek legal counsel and compliance advice to understand the implications of signing such agreements.

J. Expanding the Perimeter: Third-Party and External Stakeholders

Modern whistleblowing legislation (notably the EU Whistleblowing Directive) recognizes that misconduct is often visible to those outside the immediate payroll. Consequently, the legal "Shield of Protection" is extended to a comprehensive list of stakeholders who acquire information in a professional context.

The EU Whistleblower Directive expressly requires reporting channels to be made available to suppliers, contractors, subcontractors, consultants, agents, and self-employed people.

Many EU Member States' laws explicitly require or expect third-party access:

- **France (Sapin II / Loi Waserman)** – covers contractors and external collaborators
- **Germany (Hinweisgeberschutzgesetz)** – applies to suppliers and service providers
- **Netherlands** – extends to third parties
- **Spain (Law 2/2023)** – protects contractors, suppliers, and facilitators
- **Slovenia (Whistleblower Protection Act) -** protects a broad range of persons who are connected with the organization through work or business relationships, for example: applicants in a recruitment process, self-employed persons, partners and shareholders, members of the management board, supervisory board, or other management or supervisory bodies, volunteers and trainees, persons working under the supervision and direction of contractors, subcontractors, or suppliers. Additionally protected people are: facilitators (persons who assist the reporting person), relatives or colleagues who may be exposed to retaliatory measures, legal entities connected with the reporting person (e.g. a company owned by the reporting person).

Investors and customers increasingly expect ethical supply chains, worker voice mechanisms and human-rights grievance channels. A third-party hotline supports ESG ratings, reduces litigation and NGO pressure and demonstrates responsible business conduct.

J.1. The extended list of protected stakeholders

Stakeholder Category	Context of Disclosure	Key Rights & Protections
Outsourced Providers	IT support, KYC/CDD providers, or cloud services.	Protection against contract termination and "blacklisting" in the industry.
Self-Employed / Contractors	Independent consultants, auditors, or temporary specialists.	Right to civil damages for loss of future earnings if the relationship is cut.

Suppliers & Vendors	Entities providing goods or non-financial services.	Protection against "commercial retaliation" (unjustified withholding of payments).
Former Employees	Individuals who discover breaches during past employment.	Protection against negative references or "bad-mouthing" to future employers.
Job Applicants	Individuals who witness misconduct during the recruitment process.	Protection against discriminatory hiring practices for reporting.
Shareholders & Board Members	Persons in a supervisory or ownership capacity.	Protection against removal from office or dilution of rights for reporting.
Facilitators	Colleagues or relatives of the reporter who assist in the disclosure.	Secondary protection against "retaliation by association."

J.2. Mechanism of awareness: ensuring reach

As a Senior Compliance Officer, you cannot simply wait for these stakeholders to find your policy. You have an affirmative duty to ensure they are **aware** of their rights and your channels.

Concrete measures to ascertain awareness include:

- **Contractual "Whistleblowing Clauses":** Every Service Level Agreement (SLA) and vendor contract should include a mandatory clause detailing the firm's whistleblowing channel and the protections afforded to the provider.
- **The External Portal:** Your whistleblowing platform must be accessible from the **public-facing** website (e.g., in the footer of the webpage), not just hidden behind an internal intranet or SSO (Single Sign-On) login.
- **Vendor Onboarding Kits:** Include a "Code of Conduct for Third Parties" in every onboarding pack, explicitly highlighting the right to report without fear of commercial repercussions.
- **Public Statements:** An annual "Integrity Statement" published on the company website that explicitly invites all stakeholders—past and present—to utilize the reporting lines.

J.3. The MLRO's Verification Duty

To "ascertain" that these groups are aware, the Compliance function should perform periodic **Effectiveness Testing**:

1. **Vendor Surveys:** Sending anonymous surveys to key outsourced partners asking if they are aware of the firm's reporting channels.
2. **Audit of Contracts:** A quarterly spot-check of new contracts to ensure the mandatory whistleblowing language is present.
3. **Analytics Review:** Monitoring the "Traffic Source" of reports. If 100% of reports are internal, it may indicate that your external stakeholder awareness program is failing.

J.4. The Strategic Necessity: Why Third-Party Reporting Matters

Limiting whistleblowing to internal employees creates a "blind spot" that can be fatal for a regulated firm. In modern finance, where critical functions—from KYC/AML screening to cloud data storage—are increasingly outsourced, the most significant risks often lie just beyond the direct visibility of the Board.

J.4.1. Capturing "Outsourced Intelligence"

Third-party providers often have a more objective, bird's-eye view of your firm's operations.

- **Early Detection of Systemic Risk:** An outsourced IT provider might notice unauthorized data access patterns that internal teams have overlooked.
- **Identifying Vendor Corruption:** A secondary supplier may witness a primary contractor offering kickbacks to one of your procurement officers.
- **Neutrality:** Unlike employees, third-party stakeholders are less likely to be influenced by internal "office politics" or the "groupthink" that can sometimes suppress a report within a specific department.

J.4.2. Closing the Regulatory "Liability Gap"

Regulators (such as the FCA or EBA) hold the licensed firm responsible for the conduct of its outsourced partners.

- **Vicarious Liability:** If an outsourced KYC firm fails to flag a sanctioned individual, *your* institution faces the fine.
- **The "Reasonable Procedures" Defense:** By providing third parties with a direct line to your MLRO, you demonstrate "Adequate Procedures" under laws like the UK Bribery Act. It proves the firm has taken proactive steps to ensure integrity across its entire business ecosystem.

J.4.3. Deterrence and "Value chain" integrity

When vendors and partners know that your whistleblowing channel is open and protected, it changes the power dynamic:

- **Supplier Accountability:** Knowing that their own employees can report misconduct directly to the client (you) acts as a powerful deterrent against a vendor cutting corners or engaging in unethical practices.
- **Reputational Protection:** It prevents a scenario where a third-party witnesses wrongdoing and, feeling they have no "safe" way to tell you, goes directly to the press or the regulator, resulting in a public scandal that could have been managed internally.

J.4.4. Data-Driven Compliance

Third-party reports provide a unique data set for the MLRO. By analyzing reports from external stakeholders, you can identify **thematic weaknesses** in your onboarding processes or vendor management frameworks that internal audits might miss.

MLRO Insight: A whistleblower from a third party is often the "canary in the coal mine." They are positioned in the gaps between your internal controls, making their voice one of the most valuable assets in your risk-management toolkit.

This section moves the conversation from "legal compliance" to "business intelligence." It frames third-party reporting as a competitive advantage that protects the firm's balance sheet and regulatory license.

J.5. Navigating Cross-Border Challenges

In a globalized financial landscape, the "reporting perimeter" often crosses national boundaries. For an MLRO, this introduces a complex web of conflicting laws—where the mandatory reporting requirements of one country might clash with the strict privacy or labor laws of another.

When a whistleblowing case involves multiple jurisdictions, the investigation ceases to be a straightforward internal matter and becomes a high-stakes legal balancing act. For firms operating across borders, "compliance" in one region can inadvertently lead to "non-compliance" in another.

J.5.1. The Conflict of Laws: Transparency versus Privacy

The most significant hurdle in cross-border whistleblowing is the friction between **mandatory disclosure** and **data protection (GDPR)**.

- **The GDPR Barrier:** Transferring the personal data of a "subject" or a whistleblower from an EU branch to a non-EU headquarters (e.g., in the US or Asia) can trigger severe privacy violations unless specific "Standard Contractual Clauses" (SCCs) or adequacy decisions are in place.
- **Local Secrecy Laws:** In certain jurisdictions, "Bank Secrecy" or "State Secret" laws may prohibit an employee or third party from sharing specific documents with an international head office, even if those documents prove a major fraud.

J.5.2. Navigating Blocking Statutes

Some countries have "Blocking Statutes" designed to prevent local information from being used in foreign legal proceedings.

- **The MLRO Dilemma:** If your office in Gibraltar requires data from a subsidiary in a jurisdiction with a blocking statute, you may find yourself unable to complete a forensic audit without risking criminal charges against the local staff in that subsidiary.
- **Solution:** Firms must establish **Localized Triage**. Reports should be handled by local compliance officers first, who then provide "de-identified" or "aggregated" summaries to the central MLRO to ensure global oversight without breaching local data-export bans.

J.5.3. Handling different cultural and legal thresholds

"Wrongdoing" is not a universal concept. What constitutes a reportable offense in Northern Europe might be viewed as "standard business practice" in other regions.

- **Varying Definitions of Retaliation:** A whistleblower protected in the EU might find that their colleagues in a non-EU branch are not bound by the same anti-retaliation standards, leading to "fragmented protection" across the group.
- **Reporting Incentives:** In the US, whistleblowers can receive financial "bounties" (rewards), whereas, in many European jurisdictions, this is culturally and legally discouraged. This can lead

to "forum shopping," where a whistleblower chooses to report to a foreign regulator rather than their own internal MLRO to seek a payout.

J.5.4. Best practices for cross-border integrity

To mitigate these risks, the MLRO should ensure the following:

- **Centralized Policy, Decentralized Investigation:** Maintain one global whistleblowing policy to ensure a unified "Tone at the Top," but allow for local legal counsel to review investigation steps to ensure compliance with local labor and privacy laws.
- **Inter-Group Data Transfer Agreements:** Ensure that all subsidiaries have signed intra-group agreements that specifically cover the sharing of whistleblowing information.
- **Jurisdictional Mapping:** Maintain a "Risk Map" that identifies which countries in your network have strict data-blocking or banking secrecy laws, allowing you to tailor your investigation protocols in advance.

By addressing cross-border challenges, the MLRO demonstrates a "Senior Management" level of sophistication. It shows that the firm's framework is not just designed for a single office, but is a robust, "multi-theatre" defense system capable of protecting a complex, international entity.

J.6. Stakeholder Access Models: Engineering the Entry Points

To ensure that the "reporting perimeter" is truly inclusive, a company must provide accessible, secure, and intuitive entry points for stakeholders who do not have access to the internal corporate intranet. For a Senior Compliance Officer, the goal is to eliminate any friction that might prevent a third party from coming forward.

An effective whistleblowing framework must accommodate a wide range of technical capabilities and privacy requirements. Whether the stakeholder is a high-level consultant or a driver for a logistics partner, the "door" to the reporting channel must be easy to find and open.

J.6.1. Whistleblowing channels

The different existing channels are:

Model	Description	Primary Audience
The Public Web Portal	A dedicated, encrypted URL hosted by an independent third-party provider (SaaS).	All external stakeholders (Suppliers, Candidates, Partners).
The Direct "Hotline" (Voice)	A multi-language, 24/7 telephone service with live operators or secure voicemail.	Field workers, contractors, or those without reliable internet access.

The Hybrid "Omni-Channel"	Integration of QR codes on physical site notices, mobile apps, and dedicated email addresses.	Warehouse staff, site visitors, and mobile contractors.

J.6.2. The external SaaS Portal (the “Gold Standard”)

The most secure method is a web-based portal managed by an external vendor. It allows for a "secure postbox" where the whistleblower can return to check for messages from the compliance department /MLRO using a unique case ID and password, without ever revealing their identity or email address.

The footer of the company’s corporate homepage and/or within the "Sustainability" or "Compliance" sections is usually used to promote a clear link titled "Speak Up" or "Integrity Line".

J.6.3. QR Code & Physical Signage

For companies with physical operations (factories, construction sites, or retail branches), digital links are often insufficient. Therefore, placing posters in communal areas or "Visitor Check-in" points with a QR Code is recommended. This allows a third-party contractor to scan the code with their personal smartphone and be taken directly to the secure reporting portal instantly.

J.6.4. The Managed Hotline (the human element)

Some stakeholders feel more comfortable speaking to a human being than typing the allegations into a form. Companies can provide a toll-free number that is answered by an independent third party. This removes the fear that an "internal" person might recognize the caller's voice or phone number.

Ascertaining Awareness: The “Digital Handshake”

Providing the channel is only half the battle; the other half is ensuring the stakeholder knows it exists.

- Onboarding Integration: For every new supplier or outsourced partner, the "Access Model" should be part of the initial onboarding digital workflow. A partner should not be able to "complete" their set-up without acknowledging they have received the link to the reporting channel.
- The "Ethics Link" in Email Signatures: A simple but effective measure is to have a standardized link to the whistleblowing portal in the email signatures of the Procurement and Legal departments.
- Annual Vendor Attestation: Once a year, send a digital "Integrity Pulse" to all active third parties, reminding them of the access models and reaffirming the non-retaliation policy.

Technical Security: The “Air-Gap”

Regardless of the model chosen, the most critical technical measure is ensuring the system is external to the company network. If a third party uses a reporting tool hosted on your own servers, their IP address and traffic logs are visible to your IT department. Using an external SaaS model ensures a "Technical Air-Gap" that guarantees anonymity.

This section provides the "How-To" for the Board. It moves away from the legal "why" and into the tactical "how," showing that the company has considered the practicalities of how a delivery driver or a remote IT consultant would actually reach the Compliance department.

K. Strategic Awareness: Educating and Empowering Stakeholders

Raising awareness is not a one-time "broadcast"; it is a continuous cycle of education. We categorize this effort into three pillars: **Internal Saturation**, **External Integration**, and **Operational Verification**.

K.1. What stakeholders need to know ("the content")

Awareness campaigns must distill complex legal jargon into three clear messages:

- **The "What":** A clear definition of reportable misconduct vs. personal grievances (referencing the "Line in the Sand" from F2/F3).
- **The "Rights":** A guarantee of anonymity, confidentiality, and the absolute prohibition of retaliation.
- **The "How":** Step-by-step instructions on using the access models (Web, Hotline, or QR).

K.2. Deployment strategies by stakeholder group

Stakeholder Group	Awareness Mechanism	Frequency
Employees	Mandatory E-learning, "Town Hall" briefings and office posters	Annual /Upon induction
Senior Management	Executive workshops focusing on "Liability and duty of care".	Bi-annual
Outsourced Partners	Dedicated "Vendor Portals" and clauses in Service Level Agreements	At onboarding/contract renewal
Suppliers/Vendors	"Code of Conduct" mailshots and QR codes on delivery /access points	Annual integrity pulse
The Public/Former staff	Public-facing "Ethics Page" on the corporate website	Permanent/always accessible

K.3. Concrete measures for maximum visibility

K.3.1. The "Digital nudge"

- **Mandatory Desktop Wallpapers:** Periodic updates to corporate screensavers or intranet banners that feature the "Speak Up" hotline number and a brief message on non-retaliation.
- **Email Signature Footers:** Including a "Reporting Integrity" link in the signatures of the HR, Legal, and Procurement departments to normalize the channel.

K.3.2. Physical "safe spaces"

- **QR Code Deployment:** Placing discreet QR code stickers in breakrooms, elevator banks, and visitor lobbies. This allows a stakeholder to "capture" the link privately and revisit it later on their personal device.
- **Wallet Cards:** Distributing physical or digital "integrity cards" during induction that summarize the reporting steps.

K.3.3. Targeted vendor training

- **The "Supplier Ethics Webinar":** Hosting annual webinars for key third-party partners to explain how their staff can report concerns about your company's behavior (or their own) without risking the commercial contract.

K.4. Ascertaining awareness: the compliance officer /MLRO verification

How do you prove that people know their rights? We are moving from "Distribution" to "Confirmation":

- **The "Knowledge Audit":** Inclusion of two or three simple questions in annual employee engagement surveys (e.g., *"Do you know where to find the whistleblowing portal?"* or *"Do you believe the company would protect you if you reported misconduct?"*).
- **Read-Receipt Attestations:** Using the Compliance Management System to track who has opened and acknowledged the latest version of the Whistleblowing Policy.
- **Mystery Reporting (Testing):** Occasionally engaging a third party to "test" the hotline or portal to ensure the response times and intake quality meet the standards advertised in the awareness materials.

Awareness is the most effective deterrent against the "Payback Pitfall." When everyone knows that the system is professional, forensic, and focused on public interest, disgruntled actors are less likely to attempt to weaponize it, and genuine whistleblowers feel empowered to protect the firm.

K.5. Oversight & Governance across the supply chain

For a Senior Compliance Officer and MLRO, oversight doesn't stop at the office door. In a modern financial ecosystem, "Oversight & Governance" must be extended across the entire supply chain to ensure that your third-party partners aren't just paying lip service to ethics but are actively maintaining the same standards you uphold internally.

In an interconnected business environment, a company's risk profile is inextricably linked to the integrity of its partners. Effective governance requires moving beyond a "trust-based" model to a "verification-based" model, ensuring that whistleblowing protections and mechanisms are robustly implemented across all outsourced functions and supply chain tiers.

K.5.1. The Governance Framework: Three Pillars of Control

To maintain oversight, the Compliance function must implement a governance structure that monitors the "health" of the whistleblowing ecosystem beyond the parent company.

- Pillar 1: Contractual Accountability (The Foundation): Governance begins with the "Right to Audit" clause. Contracts must ensure that third parties maintain their own internal reporting channels or, alternatively, provide their staff with clear access to the parent company's portal.
- Pillar 2: Data Integration (The Intelligence): The MLRO should receive periodic, de-identified reports from key outsourced partners regarding the number and nature of disclosures made within their organizations that could impact the parent firm.
- Pillar 3: Active Supervision (The Verification): Governance is maintained through "Compliance Due Diligence" (CDD) at the onboarding stage and during annual reviews, treating whistleblowing maturity as a key risk metric.

K.5.2. Managing the "Outsourced risk"

When a critical function (e.g., KYC, IT, or Payment Processing) is outsourced, the risk of misconduct is also outsourced. Governance must ensure that there is:

1. Direct Escalation Paths: Third-party employees must have a "Bypass Clause" allowing them to report directly to the parent company's MLRO if they believe their own management is suppressing a report.
2. Incident Management Coordination: If a whistleblower at a third-party firm reports a breach involving your company's data or assets, there must be a pre-agreed "Joint Investigation Protocol" to ensure evidence is preserved and confidentiality is maintained across both entities.

K.5.3. Monitoring effectiveness: governance metrics

To provide the Board with assurance, the MLRO should track specific Key Performance Indicators (KPIs) across the supply chain:

- Reporting Volume by Vendor: Identifying "silent" vendors who may be suppressing reports or "high-activity" vendors who may have systemic cultural issues.
- Awareness Completion Rates: Tracking the percentage of third-party staff who have completed mandatory whistleblowing training.
- Retaliation Assessments: Reviewing any "Contract Terminations" involving individuals who previously acted as whistleblowers to ensure no retaliatory "blacklisting" occurred.

K.5.4. The Role of internal audit

A robust governance model includes Whistleblowing as a standing item in the Internal Audit plan. This includes:

- "Stress Testing" the External Portal: Ensuring the third-party access models (QR codes, hotlines) are functional and localized for the regions where the supply chain operates.
- Vendor Site Visits: Conducting spot-checks during vendor audits to ensure that "Speak Up" posters and information are physically visible in their workspaces.

MLRO Strategic Note: Governance is not about micromanaging your partners; it is about creating a "Mutual Integrity Pact." By overseeing the supply chain's whistleblowing health, you protect your firm from the "Contagion Risk" of a partner's scandal and ensure that your regulatory license remains secure.

This section provides the "teeth" for the firm's third-party strategy. It shows that the company isn't just giving third parties a phone number; but it is actively auditing their culture and holding them accountable to the same high standards as it's own internal staff.

K.5.5. Annual Transparency Reporting and Disclosures to the Public

In the modern regulatory landscape, particularly within the financial sector and under ESG (Environmental, Social, and Governance) frameworks, silence is no longer considered a sign of stability. For a Senior Compliance Officer and MLRO, the Annual Transparency Report is the definitive tool to demonstrate to the public, investors, and regulators that the firm's whistleblowing ecosystem is not just a "paper policy" but a functioning, trusted mechanism.

Transparency is the ultimate validator of a compliance culture. By publishing anonymized, high-level data regarding whistleblowing activities, an organization moves beyond "internal assurance" toward "external accountability." This practice builds market confidence and serves as a powerful deterrent to would-be wrongdoers.

K.5.5.1 The Objectives of Public Disclosure

The goal of transparency reporting is to provide a "health check" of the organization's integrity without compromising the confidentiality of individuals or ongoing investigations.

- Demonstrating Trust: High reporting volumes can, counterintuitively, be a positive indicator—showing that stakeholders trust the system enough to use it.
- ESG Alignment: Publicly sharing whistleblowing metrics is a key requirement for many ESG rating agencies and institutional investors who view "Social" and "Governance" health as a prerequisite for capital allocation.
- Regulatory Proactivity: Providing clear data reduces the likelihood of "fishing expeditions" by regulators, as it proves the firm is already self-monitoring and self-correcting.

K.5.5.2 Core data categories for disclosure

A professional transparency report must be granular enough to be meaningful but aggregated enough to protect anonymity. Recommended categories include:

Metric Category	Data to Include
Volume & Intake	Total number of reports received; percentage of reports from internal vs. external stakeholders.
Thematic Breakdown	Categorization of issues (e.g., Financial Crime, HR/Grievance, Health & Safety, Data Privacy).
Substantiation Rate	Percentage of investigated cases that were "Substantiated," "Unsubstantiated," or "Inconclusive."
Action Taken	Number of disciplinary actions, process changes, or contract terminations resulting from reports.
Case Timelines	Average time taken from initial triage to final resolution.

K.5.5.3 Protecting the “Shield of Anonymity” in public reports

The MLRO must ensure that data is never presented in a way that allows for "jigsaw identification" (where small details allow the public to guess the identity of a reporter in a small department).

- Data Masking: If a category has fewer than a certain number of reports (e.g., <3), it should be grouped into an "Other" or "General" category to prevent identification.
- Focus on Outcomes, Not Narratives: Public reports should focus on the systemic improvements made (e.g., "Updated AML onboarding protocols") rather than the specific details of the misconduct.

K.5.5.4 Distribution and stakeholder engagement

The report should not be buried in a regulatory filing; it should be used as a communication tool:

- **The Corporate Website:** Hosting a dedicated "Integrity & Transparency" section where annual reports are archived.
- **The Annual General Meeting (AGM):** Using the data to brief shareholders on the firm's risk culture.
- **The Employee Town Hall:** Sharing the report internally first to show staff that their "Speak Up" efforts lead to tangible organizational change.

Senior Compliance Insight: A company that hides its whistleblowing statistics often appears to have something to conceal. A company that publishes them—even when they highlight areas for improvements show the market it has the maturity to handle the truth.

L. Psychological safety and reasons people do not speak up

L.1.1. Definition and relevance

Psychological Safety is defined as a shared belief within a team or organization that it is safe to take interpersonal risks. This concept emphasizes an environment where individuals feel comfortable expressing their thoughts, concerns, and ideas without fear of negative consequences, such as ridicule, punishment etc.

L.1.2. How psychological safety shapes reporting behavior

Psychological safety plays a crucial role in shaping reporting behavior, particularly when it comes to whistleblowing reporting. To establish and maintain psychological safety within a team or organization, several key factors need to be in place:

- **Trust and respect**: Team members must trust one another to support and respect each other's opinions and contributions.
- **Open communication**: Team members should feel encouraged to express their thoughts, concerns, and ideas without fear of being dismissed or criticized and Leaders and team members should practice active listening to validate others' contributions.
- **Supportive leadership:** Leaders should model behaviors that promote psychological safety, such as vulnerability, openness, and actively solicit feedback and show appreciation for it, reinforcing that input is valued.
- **Emotional safety:** a culture should be created where emotional expressions are met with understanding and compassion so that employees feel safe to express their emotions, concerns, and vulnerabilities.
- **Encouragement of risk taking and innovation**: companies should foster a culture that encourages experimentation and exploration without fear of failure.
- **Inclusive practices:** companies should implement practices that ensure everyone has an equal opportunity to participate and be heard and different and diverse viewpoints are celebrated.
- **No Retaliation Policy**: individuals should not be retaliated against for speaking up about issues or concerns.
- **Focus on Learning**: Encourage a mindset that views mistakes as opportunities for learning rather than reasons for punishment.

Psychological safety does not come on its own, but rather managers and team leaders need to intentionally take several concrete steps:

Step 1: Set Clear Expectations

- **Define Psychological Safety**: Communicate what psychological safety means and why it is important for the team.
- **Establish Ground Rules**: Create ground rules for communication and collaboration that emphasize respect, openness, and constructive feedback.

Step 2: Foster Open Communication

- **Regular Check-Ins**: Schedule regular one-on-one and team check-ins to create opportunities for team members to share their thoughts and feelings.

- **Use Collaborative Tools**: Leverage communication platforms (Microsoft Teams, etc.) that encourage open dialogue and allow team members to express themselves freely.

Step 3: Model Vulnerability

- **Share Your Experiences**: Be open about your own challenges and mistakes, demonstrating that it's okay to be imperfect.

- **Encourage Sharing**: Invite team members to share their own experiences and challenges, reinforcing that vulnerability is a strength.

Step 4: Actively Listen

- **Practice Active Listening**: Show genuine interest in team members' contributions by listening without interrupting and asking clarifying questions.

- **Acknowledge Contributions**: Recognize and validate the ideas and feelings expressed by team members to reinforce their importance.

Step 5: Create Safe Spaces for Discussion

- **Anonymous Feedback Channels**: Implement anonymous surveys or feedback tools where team members can express concerns without fear of repercussion.

- **Dedicated Discussion Time**: Allocate time in meetings specifically for discussing concerns, suggestions, or ideas, ensuring everyone has a chance to contribute.

Step 6: Encourage Feedback and Input

- **Solicit Feedback Regularly**: Actively ask for feedback on your leadership style and team processes, showing that you value team input.

- **Implement Suggestions**: When feasible, act on the feedback received to demonstrate that you take team members' input seriously.

Step 7: Recognize and Reward Contributions

- **Celebrate Successes**: Acknowledge individual and team accomplishments, no matter how small, to foster a sense of belonging and recognition.

- **Reward Risk-Taking**: Encourage innovation by recognizing team members who take risks or propose new ideas, even if they fail.

Step 8: Provide Support and Resources

- **Mental Health Resources**: Provide access to mental health resources and support systems to help team members manage stress and maintain well-being.

L.2. Common reasons employees do not speak up

There are numerous reasons why employees do not speak up or report misconduct. Here are a few reasons.

L.2.1. Fear of retaliation

When employees fear that speaking up will lead to negative repercussions in their career (e.g. punishment, demotion, loss of job security) they might be hesitant to speak up.

L.2.2. Distrust in company leadership

If there is distrust in leadership and employees do not trust that their leaders will handle their concerns appropriately, they are less likely to speak up.

L.2.3. "Nothing will change" or "it does not matter" sentiment

If employees believe that their feedback or concerns will not lead to any meaningful change, they may choose to remain silent. In addition, the sense that their opinions do not matter can discourage employees from coming forward.

L.2.4. Concerns about confidentiality

If employees doubt whether their concerns will be kept confidential, they will be reluctant to come forward and report misconduct.

L.2.5. Language and cultural differences

In some cultural settings challenging the leader is usually not challenged, therefore in such setting employees will likely not Speak up.

L.2.6. Cultural stigmas

Team or departmental dynamics whereby silence is the norm and speaking up or being a whistleblower is considered "snitching", employees in such teams might feel that speaking up is not valued or even not acceptable and they will worry that by speaking up they will disrupt team harmony or will be perceived as disloyal.

L.2.7. Lack of clarity on what /how to report

In most organizations the channels to be used to report misconduct are clearly communicated. However, if there are no easily accessible channels and employees find it hard to find them, then highly likely they will not "go the extra mile" to report misconduct.

L.2.8. Fear of being wrong or ridiculed

Some employees may be hesitant to speak up if they are unsure about the facts or details of a situation, fearing they may be incorrect. The fear might even be combined with the fear of being judged or ridiculed for their ideas or opinions resulting in not speaking up.

L.2.9. Perceived personal cost versus organizational benefit

If employees believe that the perceived cost of speaking up is too high versus the benefit for the company, they might decide not to report misconduct or speak up.

L.3. Organizational drivers of silence

Within an organization there are multiple factors ("drivers") that are not beneficial for employees to speak-up.

L.3.1. Toxic or authoritarian leadership styles

A culture where employees' mental and physical well-being is not prioritized is considered a toxic culture. Signs of a toxic culture can be employees that feel overworked, unappreciated, undervalued

and leadership styles where bullying, harassment or discrimination is tolerated and where trust and respect is poor.

L.3.2. "Shoot the messenger" culture

The "shoot the messenger" culture in whistleblowing refers to the tendency of (senior) management to blame or penalize individuals who in good faith report misconduct, report violations of code of conduct, unacceptable behavior or safety hazards. This culture can have serious consequences- employees feel they are not taken seriously, feel demoralized creating an erosion of trust within the organization resulting in misconduct or violations of policy no longer being reported.

Rather than promoting a "shoot the messenger" culture, organizations should foster an environment where reporting issues are encouraged and valued, and all reporting issues are taken seriously and thoroughly investigated.

L.4. Measuring psychological safety

By employing certain measurement methods, organizations can gain valuable insights into the state of psychological safety within their teams. Regular assessment and analysis can help identify areas for improvement, fostering a culture where employees feel safe to speak up and contribute to the organization's success.

L.4.1. Employee surveys and speak-up indexes

Companies should conduct regular employee surveys that include specific questions about psychological safety. Questions may focus on whether employees feel comfortable speaking up, sharing feedback, and expressing concerns without fear of negative consequences. Companies should consider developing a "Speak-Up Index" that quantifies employees' willingness to voice their opinions. This index can be derived from survey responses and can track changes over time.

"I feel safe to speak up about my ideas and concerns."; "My opinions are valued by my team."; "I believe that my organization takes my feedback seriously." Etc. are some of the survey questions that can be used.

L.4.2. Incident data analysis vs organizational size

The company should analyze the frequency and nature of reported incidents across different countries, divisions, departments or teams and compare the reported incidents by size of the organization with the aim of seeing whether smaller groups reported more than larger organizational units.

L.4.3. Quality of reports (not just quantity)

Companies should not just evaluate the number of reports made but also the quality and depth of the information provided. High-quality reports often indicate a higher level of psychological safety.

L.4.4. Monitoring subtle retaliation indicators

Companies should monitor for subtle signs of retaliation that may indicate a lack of psychological safety, such as exclusion from team activities, negative performance reviews after reporting, or changes in behavior from colleagues. Another source of information would be to use exit interviews to gather information from departing employees about their experiences related to psychological safety and any perceived retaliation.

An increased turnover rate among employees who have spoken up would be an alarming indicator.

L.5. Legal Restrictions on speaking up

There are various legal restrictions that might prevent employees becoming whistleblowers and reporting misconduct.

L.5.1. Bank Secrecy

Financial institutions are often subject to bank secrecy laws, which require them to keep customer information confidential. Employees may face legal repercussions if they disclose this information without appropriate authorization.

L.5.2. Confidentiality agreements

Employees who have signed NDAs are legally bound to keep certain information confidential. Violating these agreements can lead to legal action from the employer. Also sharing proprietary information or trade secrets without authorization can result in legal consequences under laws protecting intellectual property.

L.5.3. Whistleblower protection laws

While whistleblower protection laws exist to encourage reporting of misconduct, there may be specific procedures that must be followed to qualify for protection. Failure to adhere to these procedures may limit legal protections. In addition, whistleblower protections may vary by jurisdiction and may not cover all types of misconduct, leading to uncertainty about what can be reported without facing repercussions.

L.5.4. Employment agreements

In some jurisdictions, employees can be terminated for any reason, including speaking up. This can create a chilling effect where employees hesitate to report issues.

L.5.5. Professional regulations

Certain professions (e.g., lawyers, doctors, accountants) have ethical and legal obligations to maintain confidentiality regarding client information. Violating these obligations can result in professional sanctions or loss of licensure.

L.6. Cultural differences in whistleblowing & Global speak-up behavior

Whistleblowing is highly culture dependent. What feels normal in one country may feel taboo in another. Cultural norms affect whether employees perceive reporting as loyalty or betrayal, trust internal systems, expect retaliation or feel empowered to question authority

L.6.1. Power Distance

Countries with high power distance (e.g. Mexico and Brazil in Latin America, Saudi Arabia and UAE in Middle East, Malaysia and Indonesia in Asia or Russia) exhibit significant disparities in power and authority between individuals at different levels within organizations and society and therefore tend to have a speak-up culture that is less supportive of open communication and dissent.

In high power distance cultures, communication tends to flow from the top down. Employees may feel that it is inappropriate to question or challenge authority, leading to a reluctance to speak up and believing that their opinions or concerns are less valuable than those of higher-ranking individuals. Decisions are often made by those in authority without input from lower-level employees, which can lead to a culture were speaking up is not encouraged or valued.

L.6.2. Collectivism versus Individualism

Individualist cultures (Sweden, Norway, UK, Netherlands) emphasize personal autonomy and individual rights, value self-expression, independence, personal achievement and individuals are encouraged to voice their concerns and Speak up. In collective cultures (Greece, Italy, Spain, Poland, Russia) the emphasis is on group harmony, loyalty, group consensus, and relationships and the group needs are prioritized over individual needs.

In individualist cultures employees feel a sense of personal responsibility to report wrongdoing, viewing it as an ethical obligation to themselves and others. In collectivist cultures there is hesitation to speak up due to concerns about disrupting group harmony or causing conflict.

L.6.3. Uncertainty avoidance

Uncertainty avoidance is a cultural dimension identified by Geert Hofstede, which reflects the degree to which individuals in a society feel uncomfortable with uncertainty and ambiguity.

Individuals in high uncertainty avoidance cultures (Greece, Portugal, Spain, Hungary) tend to prefer clear rules, structured environments, and predictable outcomes, there is often a strong emphasis on group harmony and consensus. They also have a strong aversion to ambiguity, and people often seek security and stability. Employees may avoid blowing the whistle to maintain team cohesion.

Individuals in low uncertainty avoidance cultures (UK, Sweden, Denmark) are generally more comfortable with ambiguity and uncertainty. Such individuals are more willing to take risks associated with reporting misconduct, as they may perceive the potential benefits (e.g., ethical integrity, organizational improvement) as outweighing the risks.

L.7. How can companies adapt globally and create psychological safety?

There are various initiatives companies can or should take.

L.7.1. Tailor training to cultural expectations and norms

Develop training programs that are culturally relevant (Cultural Sensitivity) and consider local values, communication styles, and norms. This ensures that employees understand the importance of psychological safety in a way that resonates with their cultural context.

L.7.2. Use local champions to promote speak-up culture

Companies should engage respected leaders or influential figures within local teams to champion the importance of psychological safety and the speak-up culture. Such local champions can help bridge cultural gaps, making it easier for employees to relate to the message and feel empowered to speak up.

L.7.3. Offer multiple reporting channels

Companies should ensure that reporting channels are accessible and culturally appropriate, considering factors such as language and local customs. Moreover, companies should provide various channels for reporting concerns, such as anonymous hotlines, online platforms, and in-person options. This accommodates different preferences and comfort levels among employees.

L.7.4. Translate policies not just linguistically- but also culturally

Companies should culturally adapt their policies i.e. Go beyond mere translation of policies to ensure they align with local cultural values and practices. This includes adapting the tone, examples, and implications of the policies to fit the cultural context.

L.7.5. Reinforce non-retaliation protection visibly and repeatedly

Companies should regularly communicate the organization's commitment to non-retaliation policies through various channels (e.g., meetings, newsletters, and training sessions) and employees should see tangible outcomes when they report concerns, otherwise they lose trust in the system.

M. What are some of the challenges for whistleblowers before, during and after the Disclosure?

Before a disclosure is ever made, whistleblowers often endure a period of intense internal conflict and psychological "pre-reporting" stress. The primary challenge at this stage is the weighing of moral obligation against the very real fear of professional suicide or social isolation. Prospective reporters must navigate the "bystander effect" and the daunting task of gathering sufficient evidence without detection, often while questioning their own perception of reality in the face of institutional gaslighting. This phase is characterized by a profound sense of loneliness as the individual evaluates whether the organization's internal channels are a genuine safety net or a trap designed to identify and neutralize "troublemakers."

During and after the disclosure, the challenges shift from internal psychological battles to external, systemic pressures. During the investigation, whistleblowers often face "limbo," where they are sidelined from key projects or subjected to subtle "gray rocking" by peers and management who fear association with them. Once the process concludes—regardless of the outcome—the "after-effects" can be devastating, including the «blacklisting» within an industry, protracted legal battles over retaliation, and a permanent shift in their professional identity. Even when legally protected, the "social stigma" of being a whistleblower can lead to long-term career stagnation and "injury to feelings," requiring immense personal resilience to transition back into a stable professional life.

M.1. The Pre-Disclosure Barrier: The "Silent Struggle"

For a Senior Compliance Officer, understanding the pre-disclosure phase is vital. If the barriers at this stage are too high, the most expensive reporting software in the world will remain empty. This phase is defined by a "silent struggle" where the potential whistleblower is often their own harshest interrogator.

Before a report is ever filed, a prospective whistleblower undergoes a grueling period of internal deliberation. During this time, the individual is not just a "reporter," but a person trying to protect their livelihood, their social standing, and their mental health.

M.1.1. The Psychological "Weight of proof"

The most immediate challenge is the Subjective Burden of Proof. Prospective whistleblowers often agonize over whether what they have witnessed is "enough" to report.

- Self-Doubt and Gaslighting: They may question their own interpretation of events, especially if the misconduct is subtly woven into "standard business practice."
- «Am I Wrong?" Loop: Without a trusted confidant, the individual may feel they are overreacting, leading to significant anxiety and "paralysis by analysis."

M.1.2. Fear of "Institutional Trap”

A primary deterrent is the lack of trust in the **integrity of the channel**.

- **Anonymity Anxiety:** The fear that "anonymous" doesn't truly mean anonymous—that the IT department or a senior manager will be able to trace the report back to them via metadata, IP addresses, or writing style.
- **The "Company Man" Conflict:** A deep-seated fear that the Compliance department is merely a "shield for the Board" and that reporting will result in the company protecting the perpetrator while "purging" the reporter to maintain the status quo.

M.1.3. The “social cost” of integrity

Humans are social creatures, and the threat of **ostracization** is a powerful deterrent.

- **Fear of Being the "Snitch":** The pervasive cultural stigma against "tattling" can make an employee feel that by reporting, they are betraying their team or their friends.

- **The Bystander Effect:** Seeing others ignore the misconduct can lead a prospective whistleblower to believe that since no one else is speaking up, they shouldn't either—fearing they will be seen as the "odd one out."

M.1.4. Professional and Economic precarity

For many, the decision to blow the whistle is weighed against their financial survival.

- Mortgage and Family Pressure: The realization that being "pushed out" could lead to a loss of income, healthcare, and future employability.
- Career Suicide: In niche industries (like specific areas of high-frequency trading or specialized legal services), the fear that being known as a whistleblower will lead to a quiet, industry-wide "blacklisting" that ends their career permanently.

M.1.5. Information Gathering Dilemma

Finally, the individual faces a tactical challenge: How to prove the breach without getting caught?

- Access Risks: Trying to secure copies of emails or transaction logs without triggering "data exfiltration" alerts.
- The "Mole" Feeling: The intense stress of acting as a "covert agent" within their own team, which can lead to burnout and erratic behavior even before the disclosure is made.

M.2. Challenges During the Disclosure: The "Eye of the Storm"

Once the whistleblower hits "send" or picks up the phone, the nature of their struggle shifts from internal deliberation to external navigation. This "Middle Phase" is often the most volatile, as the individual is forced to function within an organization that is now effectively a "crime scene" under active investigation.

During the investigation, the whistleblower enters a state of professional and psychological limbo. While the MLRO and investigators are focused on the facts, the whistleblower is often navigating a deteriorating work environment and a complex procedural maze.

M.2.1. The “Silo effect” and professional isolation

Even when confidentiality is strictly maintained, a "vibe" often permeates the department.

- **The "Gray Rock" Treatment:** Colleagues who suspect a disclosure has been made may stop inviting the individual to lunch, "forget" to include them on email chains, or become suddenly formal in their interactions.
- **Sidelining:** Managers—sometimes unintentionally—may stop assigning high-profile projects to the whistleblower to "reduce their stress," which the individual perceives as the beginning of their professional erasure.

M.2.2. Procedural anxiety and the “Information Vacuum”

One of the greatest challenges is the **Lack of Transparency** inherent in forensic investigations.

- **The Silence of Compliance:** Because the MLRO cannot share details of an ongoing investigation to protect its integrity, the whistleblower often hears nothing for weeks or months. This "silence" is often misinterpreted as the company doing nothing or, worse, "burying" the report.
- **Repetitive Questioning:** Being interviewed multiple times by different investigators (Internal Audit, Legal, External Counsel) can feel like an interrogation rather than support, leading to "reporting fatigue."

M.2.3. The “Double life” Syndrome

The whistleblower must continue to perform their daily duties, often sitting feet away from the person they have accused.

- **Cognitive Dissonance:** Maintaining a professional demeanor while knowing that a forensic team is currently dismantling the subject's files.
- **Fear of Accidental Disclosure:** The constant stress of "slipping up" in conversation or being seen entering the Compliance office.

M.2.4. Counter-accusations and Character Assassination

If the subject of the report discovers or suspects who the whistleblower is, they may launch a pre-emptive strike.

- **Deflection:** The subject may suddenly report the whistleblower for minor procedural infractions or "aggressive behavior" to discredit them before the investigation concludes.
- **The "Payback" Label:** The subject may try to frame the disclosure as a "personal vendetta" to steer the investigators away from the factual breach.

M.2.5. Loss of control

Once the disclosure is made, the whistleblower is no longer the "owner" of the information.

- **Shift in Narrative:** The investigators may focus on a different aspect of the breach than the one the whistleblower felt was most important.
- **Pace of the Organization:** The whistleblower may want immediate action, but the legal and regulatory "Due Process" takes time, leading to frustration and a sense of powerlessness.

M.3. Challenges After the Disclosure: The "Long Shadow"

The conclusion of an investigation rarely marks the end of the whistleblower's journey. For the MLRO, this "post-disclosure" phase is where the most significant legal risks regarding retaliation occur and where the long-term health of the firm’s ethical culture is decided.

Even when an investigation substantiates the whistleblower’s claims and corrective action is taken, the individual often faces a "new normal" that is fraught with professional and personal hurdles.

M.3.1. The “Pariah” Effect and career stagnation

The most common long-term challenge is the subtle, often unprovable, "ceiling" that is placed on the whistleblower’s career.

- **The "Snitch" Label:** Even if the whistleblower saved the company millions, they may be viewed by management as "unpredictable" or "not a team player." This leads to being bypassed for promotions or excluded from high-stakes projects.
- **Subtle Retaliation:** Managers may apply hyper-scrutiny to the whistleblower’s future work, waiting for a minor mistake to justify a "performance-based" termination that is retaliatory in nature.

M.3.2. Industry-Wide “Blacklisting”

In specialized sectors, especially the financial services industry, news travels fast.

- **The Reputation Trap:** If a whistleblower leaves the firm, they may find it surprisingly difficult to secure a new role. Recruiters or hiring managers may have "heard things," leading to a quiet exclusion from the job market.

- **Reference Anxiety:** The fear that the former employer will provide a "lukewarm" or technically accurate but damaging reference that prevents future employment.

M.3.3. Moral Injury and Psychological Fallout

The emotional toll of whistleblowing can linger for years, often manifesting as "Moral Injury"—the psychological distress caused by witnessing or failing to prevent acts that transgress deeply held moral beliefs.

- **Hyper-vigilance:** After being in a high-stress investigative environment, the individual may struggle to trust new colleagues or supervisors, constantly looking for signs of corruption or impending retaliation.
- **Post-Traumatic Stress:** The "exhaustion phase" following the adrenaline of the investigation can lead to depression, burnout, or a total loss of interest in their professional field.

M.3.4. The Burden of the “Reverse Onus”

While laws like the EU Whistleblowing Directive provide a "Reverse Burden of Proof" to protect against retaliation, the whistleblower still bears the **emotional and financial cost of litigation**.

- **Lengthy Court Battles:** Proving retaliation in court can take years. Even with a strong case, the individual must endure the stress of a public legal battle against a well-funded corporate legal team.
- **The "Pyrrhic Victory":** Winning a lawsuit for damages often feels hollow if the individual's career in their chosen field is effectively over.

M.3.5. Social and Personal Strain

The impact often ripples into the whistleblower's private life.

- **Relationship Stress:** The prolonged period of secrecy and stress during the "before" and "during" phases can strain marriages and friendships.
- **Financial Instability:** Even if the whistleblower is still employed, the fear of imminent job loss can lead to extreme financial conservatism and a decreased quality of life.

M.3.6. MLRO’s role in post-disclosure care

To mitigate these challenges, the Senior Compliance Officer must move beyond "case closed." Concrete measures include:

- **The "After-Care" Program:** Scheduling formal check-ins at 6 and 12 months post-investigation to monitor the whistleblower's career progress and mental well-being.
- **Positive Reintegration:** Ensuring that the whistleblower is publicly (or privately, depending on their preference) thanked or recognized for their contribution to the firm’s integrity, helping to reframe them as a "Hero" rather than a "Snitch."

M.4. The Whistleblower’s Guide: Professional Best practices

For a Compliance Officer, providing a "Best Practice Guide" for the whistleblower is a dual-purpose strategy: it helps the individual protect their own interests while ensuring the investigation remains untainted and forensic.

When a whistleblower acts professionally and follows a structured protocol, they significantly increase the likelihood of a successful outcome and strengthen their legal standing in the event of retaliation.

Stepping forward as a whistleblower requires a transition from "observer" to "key witness." To navigate this successfully, the individual should treat their participation as a disciplined, evidence-based project.

M.4.1. Pre-Disclosure: Establishing the Foundation

- **Stick to the Facts:** Avoid emotional language or speculation. Focus on the "Who, What, Where, When, and How."
- **Identify, Don't Exfiltrate:** Note the locations of evidence (e.g., "Email dated Jan 5th in Folder X") rather than downloading mass amounts of data to a personal drive, which could be flagged as a security breach or "theft of trade secrets."
- **Seek Confidential Counsel:** Before reporting, speak with a specialized legal advisor or a whistleblower support NGO to understand your specific statutory rights.

M.4.2. During the Disclosure: Maintaining Integrity

- **The "Cone of Silence":** Do not discuss the report with colleagues, friends at work, or on social media. Any leak on your part could compromise the investigation and provide the subject with a "due process" defense.
- **Keep a Contemporaneous Journal:** Maintain a private, off-site log of all interactions related to the report. Document any sudden changes in your workload, exclusion from meetings, or shifts in managerial tone. This is your primary evidence if you ever need to prove retaliation.
- **Be Exhaustive but Honest:** During interviews, if you don't know an answer, say so. Guessing can lead to inconsistencies that "payback" seekers will use to discredit your entire testimony.

M.4.3. Interaction with the accused

- **Maintain Professionalism:** Continue to perform your duties to the best of your ability. Do not confront the subject or change your behavior toward them.
- **Avoid "Baiting":** If the subject becomes aggressive or seeks confrontation, walk away and report the incident immediately to the MLRO. Do not engage in verbal sparring, as this can be used to label you as "difficult" or "unprofessional."

M.4.4. Post- Disclosure: Protecting the Future

- **Monitor Your Career Trajectory:** If you are bypassed for a promotion or receive a surprisingly negative performance review, formally ask for written feedback. Compare this against your history of reviews.
- **Exercise Your Right to "After-Care":** If the organization offers psychological support or "Pulse Checks," use them. These sessions create a documented record of the company's ongoing duty of care toward you.

Summary Table: The Whistleblower's "Do's and Don'ts"

DO	**DON'T**
Do keep your records on personal devices/folders (off the company network).	**Don't** use company resources (printers/scanners) to prepare your disclosure.
Do report any "subtle" changes in treatment immediately.	**Don't** try to "investigate" the case yourself after reporting.
Do cooperate fully with the Compliance team.	**Don't** expect or demand a specific punishment for the subject.
Do prioritize your mental health and seek external support.	**Don't** threaten the company with "going to the press" as a leverage tool.

By educating the whistleblower on how to be a "Good Witness." It demonstrates that the company is transparent and wants the whistleblower to be protected not just by the firm, but by their own professional conduct.

N. Protecting whistleblowers & anti-retaliation

Protecting whistleblowers is not merely a regulatory obligation; it is a fundamental pillar of sustainable corporate governance and risk management. By establishing a safe environment for reporting, companies empower their own "human sensors" to surface internal threats—such as fraud, money laundering, or systemic ethical breaches—long before they escalate into catastrophic legal liabilities or public scandals. This proactive approach allows the MLRO and senior leadership to address misconduct internally and discreetly, significantly reducing the likelihood of heavy regulatory fines, de-risking the organization, and preserving institutional value. In an era where transparency is a currency, a robust protection framework signals to investors, partners, and regulators that the firm is committed to a culture of accountability over a culture of concealment.

Furthermore, authentic whistleblower protection serves as a powerful deterrent against the "weaponization" of reporting channels by disgruntled actors. When a company demonstrates that it handles every disclosure with forensic objectivity and zero tolerance for retaliation, it builds a high level of psychological safety and trust within the workforce. This cultural integrity ensures that employees feel valued as guardians of the firm's reputation rather than targets of its hierarchy. Ultimately, by shielding those who speak up in good faith, an organization transforms a potential vulnerability into a strategic asset, fostering a resilient, ethical, and high-performing environment where long-term success is built on the bedrock of collective integrity.

As highlighted in the previous paragraphs, for a compliance culture to thrive, stakeholders must feel safe. However, as an MLRO, you must clarify that **protection is a shield, not a cloak.** It protects the honest reporter from harm, but it does not grant immunity for the reporter's own prior misconduct.

N.1. Defining prohibited retaliation

The organization strictly prohibits any adverse action taken against a person for making a *bona fide* report. This includes, but is not limited to:

- **Employment-related:** Termination, demotion, withholding of bonuses, or "blacklisting."
- **Commercial-related:** Unjustified termination of supplier contracts or withholding payments to business partners.
- **Social-related:** Bullying, isolation, or reputational smearing.

N.2. The burden of proof ("the reverse onus")

In alignment with modern European standards, if a whistleblower suffers an adverse action shortly after reporting, the **burden of proof shifts to the company**. The organization must prove that the action (e.g., a contract termination) was based on legitimate, documented performance grounds entirely unrelated to the whistleblowing report.

N.3. Limitations of protection

It is vital to draw a line regarding **immunity**:

- **Self-Reporting:** If a business partner reports a bribery scheme they were actively participating in, the act of whistleblowing does not automatically wipe away their liability. However, "active cooperation" may be considered as a mitigating factor in subsequent enforcement.
- **Malicious Intent:** Protection is strictly reserved for those with a **reasonable belief** in the truth of their report. Those found to have intentionally provided false information to harm a competitor, or supervisor will face disciplinary or legal action.

Senior Compliance Note: By clearly stating that "protection" does not equal "immunity for the guilty," we deter disgruntled parties from using the whistleblowing channel as a last-ditch effort to avoid the consequences of their own poor performance or contractual breaches.

N.4. What concrete measures must companies take to protect whistleblowers?

To transition from a policy on paper to a truly protective environment, companies must implement a multi-layered defense system that covers technical, legal, and cultural dimensions.

N.4.1. Technical & structural safeguards

- **Encrypted Reporting Channels:** Companies must provide a reporting mechanism (typically a third-party hosted platform) that allows for complete anonymity. This platform should be "air-gapped" from the company's internal IT network to ensure metadata—such as IP addresses or timestamps—cannot be traced back to a specific workstation.
- **The "Need-to-Know" Firewall:** Access to the identity of a whistleblower must be restricted to a dedicated Whistleblowing Office or the MLRO. Any unauthorized attempt to bypass this firewall or "unmask" a reporter must be treated as a severe disciplinary offense.

N.4.2. Legal & Procedural Protection

- **The Reverse Onus of Proof:** A concrete protection measure is the adoption of the "Reverse Burden of Proof." If an employee suffers an adverse action (e.g., a demotion or poor performance review) within a certain timeframe after reporting, the company must legally prove the action was entirely unrelated to the disclosure.
- **Non-Retaliation Contracts:** Including specific non-retaliation clauses in employment contracts and supplier agreements. This provides a clear legal basis for the whistleblower to seek damages if protection is breached.
- **Immunity for Procedural Breaches:** Companies should provide "Safe Harbor" protocols where a whistleblower is protected from disciplinary action for breaching internal confidentiality or data-handling policies *if* that breach was necessary to surface a legitimate regulatory violation.

N.4.3. Operational & Cultural measures

- **Interim Protective Measures:** During an ongoing investigation, the company must be prepared to offer temporary reassignments, changes in reporting lines, or paid leave to separate the whistleblower from a potentially hostile work environment or a supervisor they have accused.
- **Ongoing Monitoring (Post-Case):** Protection does not end when the investigation closes. A concrete measure is a mandatory "Check-In" protocol where the Compliance team contacts the whistleblower at 3, 6, and 12-month intervals to ensure no "subtle" retaliation (such as social isolation or exclusion from projects) has occurred.
- **Anti-Retaliation Training:** Mandatory training for middle management specifically on how to manage a team containing a whistleblower. Managers must understand that even a "cold shoulder" can be interpreted as retaliation under modern European standards.

By implementing these measures, a company shifts the risk from the **individual** to the **process**. Concrete protection is about ensuring that the person who spoke up can continue their career or business relationship without the shadow of their disclosure affecting their professional trajectory.

N.5. Preventive steps against anti-retaliation

While the previous section covered broad protection measures, preventing **retaliation** requires a more forensic, "pre-emptive strike" approach. To an MLRO, retaliation is a specific risk that must be mitigated through active surveillance and administrative controls.

Prevention is significantly more effective than remediation. Companies must treat the risk of retaliation as a "Compliance Risk" that requires active monitoring rather than a "Human Resources" issue that is handled after the fact.

N.5.1. Administrative “Segregation of Duties”

- **Conflict-of-Interest Mapping:** Immediately upon receiving a report, the Compliance team must map out the reporting lines of the whistleblower. If the subject of the report is the whistleblower's direct supervisor or a person with influence over their bonus/promotion, the company must implement an **Alternative Reporting Line** for the duration of the investigation.
- **Freeze on Personnel Actions:** A concrete preventive measure is the "Personnel Action Freeze." No changes to the whistleblower’s status (salary, location, job description, or disciplinary record) should be permitted without the explicit, written sign-off of the **Chief Compliance Officer or MLRO**. This prevents "stealth retaliation" disguised as routine management.

N.5.2. Confidentiality “Need to Know”- Protocols

- Identity Shielding: Retaliation cannot occur if the retaliator does not know who the whistleblower is. Companies must use de-identified summaries during the investigation. Instead of saying "John Doe reported X," the investigator states "A report was received regarding X."
- The "Leak" Penalty: Establishing a zero-tolerance policy for any employee who attempts to "investigate the investigator" or guess the whistleblower's identity. Making the attempt to identify a whistleblower a dismissible offense is a powerful deterrent.

N.5.3. Active “Anti-Retaliation Surveillance”

- **The "Pulse Check" Schedule:** The Compliance Department should conduct monthly "Pulse Checks" with the whistleblower. These aren't just chats; they are structured interviews asking: *“Have you been excluded from meetings? Has your workload shifted? Has the tone of your manager changed?”* * **Benchmarking Performance Reviews:** If a whistleblower’s performance rating drops suddenly following a report, the Compliance team should have the authority to audit that review against previous years to ensure it isn't being used as a retaliatory tool.

N.5.4. Managerial “Soft skills” Training and Accountability

- **Specific Managerial Briefings:** Managers of whistleblowers (who are not suspects) should be briefed on their legal duties. They must understand that "retaliation" includes passive-aggressive behavior, such as social isolation or withholding information necessary for the employee to do their job.
- **Positive Reinforcement:** Including "Contribution to Ethical Culture" as a metric in management appraisals. This ensures that managers are incentivized to protect those who speak up rather than seeing them as "troublemakers."

By implementing these measures, the organization moves from **detecting** retaliation to **pre-empting** it. This satisfies the "Duty of Care" required under the EU Whistleblowing Directive and ensures that the "line" between a disgruntled actor and a protected whistleblower remains clear: the process protects the truth, and the company protects the person who brought it forward.

N.6. The cost of failure: legal and financial consequences of retaliation

In many jurisdictions, particularly under the **EU Whistleblowing Directive** and the **UK Public Interest Disclosure Act (PIDA)**, the penalties for retaliation have shifted from administrative slaps-on-the-wrist to severe, enterprise-threatening consequences. For the MLRO, these risks represent "Unmanaged Regulatory Exposure."

N.6.1. Regulatory fines and sanctions

Regulatory bodies (such as the FCA, BaFin, or local Financial Intelligence Units) now view the failure to prevent retaliation as evidence of a "broken" compliance culture.

- **Direct Fines:** Penalties can reach millions of Euros or a percentage of global annual turnover.
- **License Revocation:** In extreme cases, a demonstrated pattern of retaliatory behavior can lead to a "fitness and propriety" review of the firm's senior management, potentially resulting in the suspension of the firm's operating license.
- **Public Censure:** Regulators often "name and shame" firms that fail to protect whistleblowers, leading to a loss of institutional trust that can take decades to rebuild.

N.6.2. Civil liability and unlimited damages

Unlike standard employment disputes, whistleblowing retaliation claims often bypass traditional "caps" on compensation.

- **Unlimited Awards:** In jurisdictions like the UK and various EU member states, if a whistleblower proves they were dismissed or "detrimentally treated" due to their disclosure, the financial award can be **unlimited**, covering full loss of future earnings, pension contributions, and "injury to feelings."
- **The "Reverse Burden" Penalty:** Because the company must prove a negative (that the action was *not* retaliatory), firms that lack the concrete measures outlined in the previous sections almost always lose these cases in court.

N.6.3. Personal liability for senior managers

Modern legislation increasingly pierces the corporate veil.

- **Individual Fines:** Senior managers, including MLROs or CEOs, who are found to have personally participated in or turned a blind eye to retaliation can face individual fines.
- **Professional Barring:** An individual found guilty of retaliating against a whistleblower may be barred from holding a "Controlled Function" or "Senior Management Function" in the financial services industry for life.

N.6.4. Reputational and strategic impact

Beyond the courtroom, the fallout is devastating:

- **"The Brain Drain":** Top talent will not work for an organization perceived as "toxic" or punitive toward integrity.
- **Investor Withdrawal:** ESG (Environmental, Social, and Governance) investors now use whistleblower protection metrics as a key "S" pillar. Evidence of retaliation can trigger immediate divestment from institutional funds.
- **Increased Scrutiny:** Once retaliation is proven, the firm is often placed under a "Monitor" or subject to permanent, high-intensity regulatory supervision.

MLRO Insight: The cost of implementing an anti-retaliation framework is a fraction of the cost of a single losing retaliation claim. Protection is not overhead; it is **litigation insurance**.

N.6.5. Which specific measures should the external authorities and governments take to ensure that whistleblowers are protected from harmful consequences?

For external authorities and governments, the objective is to create a **national safety net** that exists outside the control of any single corporation. When a company's internal protections fail, or when the

company itself is the perpetrator of the misconduct, the state must provide a secondary layer of defense.

N.6.5.1 Statutory “Safe Harbor” and Legal Immunity

Governments must provide a clear legal framework that overrides private contracts and non-disclosure agreements (NDAs).

- **Immunity from Prosecution:** Authorities must ensure whistleblowers are protected from criminal, civil, and administrative liability (e.g., for defamation, breach of copyright, or trade secret theft) provided they had reasonable grounds to believe the information was true.
- **Invalidation of NDAs:** Laws must explicitly state that any contractual clause prohibiting a person from reporting a crime or regulatory breach to the authorities is void and unenforceable.

N.6.5.2 Institutional Support: The independent oversight body

Authorities should (consider) establishing a specialized, independent agency (often called a "Whistleblowing Authority" or "Ombudsman").

- Advice and Counsel: Governments should provide free, confidential legal and psychological advice to whistleblowers.
- The "Psychological Shield": Whistleblowers often face extreme stress; state-funded counseling services ensure the individual is not "broken" by the process.
- Certification of Status: The authority can issue a "Certificate of Whistleblower Status," which acts as a legal shield the individual can present to banks, future employers, or courts to explain gaps in employment or to trigger specific protections.

N.6.5.3 Financial and Career continuity measures

To prevent a whistleblower from being "starved out" through job loss or blacklisting, governments must intervene in the economic reality of the situation.

- **Interim Relief in Courts:** Authorities must allow for "interim relief," where a court can order an employer to continue paying the whistleblower's salary while a retaliation lawsuit is pending.
- **Bounty or Reward Systems:** In some jurisdictions (like the US SEC model), the state provides a percentage of the recovered fine to the whistleblower. This compensates for the high likelihood that the individual may never work in their specific niche industry again due to blacklisting.
- **Remediation for "Blacklisting":** Governments should penalize "informal" retaliation, such as industry-wide blacklisting, by treating it as a separate criminal offense.

N.6.5.4 Physical Security and Witness Protection

When a disclosure involves organized crime, high-level corruption, or money laundering, the threat moves from professional to physical.

- **Relocation and Identity Changes:** In extreme cases, governments must be prepared to integrate whistleblowers into Witness Protection Programs.
- **Anonymity in Legal Proceedings:** Authorities must allow whistleblowers to testify or provide evidence under a pseudonym or behind a screen to prevent public shaming and targeted threats.

N.6.5.5 Punitive sanctions for retaliators

The state must ensure that the "cost of retaliation" is higher than the "cost of compliance."

- **Criminal Liability for Retaliation:** Governments should criminalize the act of retaliating against a whistleblower, moving beyond civil fines to potential prison sentences for executives who authorize such actions.
- **Reverse Onus of Proof in Legislation:** Statutory law should mandate the "Reverse Burden," forcing the employer to prove in court that an adverse action was unrelated to the whistleblowing disclosure.

N.6.5.6 Public awareness and “normalization”

Governments have a duty to change the social narrative.

- **Educational Campaigns:** Publicly framing whistleblowers as "Guardians of the Public Interest" rather than "snitches" or "traitors."
- **Public Recognition:** Establishing awards for ethical bravery to celebrate the positive impact whistleblowers have on the economy and rule of law.

N.6.5.7 Summary

From the perspective of an MLRO, this section highlights that while a company does its part, the **State** is the ultimate guarantor of safety. This creates a dual-layer system where the whistleblower is protected inside the office by the MLRO and outside the office by the Law.

O. Retaliation against Chief Compliance Officer

O.1. Forms of retaliation against Chief Compliance officer

Retaliation against a Chief Compliance Officer (CCO) can take many forms, especially when the CCO raises concerns, enforces rules, reports misconduct, or resists pressure from leadership. Retaliation is often subtle and indirect and can take any of the below forms:

- **Structural Retaliation:** eliminating CCO independence, changing reporting lines (e.g., from board to management), merging compliance into legal or operations to dilute oversight.
- **Reputational Harm:** smear campaigns or questioning integrity/competence, blaming the CCO for compliance failures they warned about, leaking negative information internally or externally.
- **Professional Isolation:** marginalization by senior leadership, loss of direct access to the board or audit committee, being ignored or overruled without explanation.
- **Undermining Authority:** Bypassing the CCO in decision-making, stripping budget, staff, or resources, excluding the CCO from key meetings or committees, reassigning compliance responsibilities to others without justification etc.
- **Performance Manipulation:** Unjustified negative performance reviews, changing performance metrics to ensure failure, documenting minor or fabricated issues to build a termination case.
- **Employment Actions:** termination or forced resignation, demotion or removal of title/authority, reduction in compensation, bonuses, unfavorable reassignment to a less influential role.
- **Psychological and Workplace Harassment:** Intimidation or bullying, hostile work environment, pressure to reverse findings or “tone down” reports.

O.2. Retaliation versus non-retaliation: key differentiators

Although the distinction between retaliation and non-retaliation is not always 100% easy to make, certain guidelines can be followed.

We can assume that more likely a retaliation is happening when:

a) compliance function or chief compliance officer is uniquely impacted (and other governance functions such as legal, internal audit or risk are not similarly impacted).

b) when an action affecting the chief compliance officer happens closely after CCO escalated to the board, reported misconduct or said no to a business initiative.

c) when CCO independence is reduced, normal governance approvals are bypassed and decisions are made informally, without documentation and without board awareness.

On the contrary when changes affecting the chief compliance officer or compliance function are applied consistently across all functions, the action was planned or budgeted before the activity by CCO, reasons given are specific, measurable and alternatives were considered, then retaliation is less likely to have happened.

O.3. Actions a chief compliance officer can take against retaliatory claims

In the case of **structural retaliation**, the CCO should document the reporting line changes and document such changes against regulatory guidance and/or industry best practice. Important though is that CCO documents his/her objections before changes are finalized by escalating this issue to the full Board. E.g. “The proposed structure compromises compliance independence and may breach regulatory expectations.”

In the case of **psychological harassment,** the CCO should keep a log of incidents and identify witnesses. Internally the CCO can escalate this as a governance and retaliation issue and mention the importance of mental health and a hostile environment.

In the case of **undermining authority**, the CCO should document the lost budget resources, headcount or decision rights, compare his/her situation with peers in similar companies, compare the situation with Regulatory Guidance and identify operational risks caused by the loss of authority. Internally the CCO can then escalate to the Board with an impact analysis, highlighting unmet regulatory expectations and requesting a formal reaffirmation of the CCO authority. Alternatively, the CCO can consider reporting the issue to the regulator.

In the case of **professional isolation**, it is recommended that CCO logs exclusions from meetings, committees, communication and/or loss of board access. The CCO should escalate to the Chairman of the Board highlighting that “Restricted access impairs my ability to meet regulatory expectations.”. and documenting his/her inability to discharge duties.

In the case of **reputational harm**, the CCO should maintain evidence of defamatory statements, false allegations, leaks etc., and ask for corrective communications if misinformation is spreading.

In the case of **employment actions** (such as termination, demotion, salary/bonus reduction), the CCO should document the timing between his/her compliance activity and adverse activity. In addition, the CCO should request written justification for the employment action and preserve all related performance reviews and relevant emails. Moreover, the CCO should escalate the adverse employment action following a compliance decision to the Board, Audit/Compliance Committee and consider hiring independent legal counsel or filing a retaliation claim.

In the case of **performance manipulation,** the CCO should document and preserve all prior (positive) performance evaluations, request specific and measurable deficiencies, respond in writing to the deficiencies and ask the Board to review the sudden change in performance and inconsistency with prior evaluations.

Important here is to realize that internal company counsel is conflicted as they would typically represent the company and not the employee /CCO. Therefore, it is recommended to engage independent counsel.

P. Challenges and opportunities in the recruitment of whistleblowers?

P.1. Why are companies not recruiting whistleblowers?

Companies often publicly promote a Speak-up culture and the importance of integrity. Whistleblowers embody exactly these values by speaking up. You would expect that companies will recruit whistleblowers, however in practice we see the opposite happening. Why is this?

There are several reasons why companies are reluctant to recruit whistleblowers.

P.1.1. Whistleblowers are seen as “high risk” employees

From a company’s perspective, a known whistleblower represents **uncertainty**. Whistleblowers have demonstrated a willingness to challenge authority and/or whistleblowers may escalate issues externally if dissatisfied internally.

Senior leaders in the organization often fear loss of control over narratives and timing.

P.1.2. Whistleblowers are associated with litigation and conflict

Many whistleblowers have histories involving legal disputes, regulatory investigations and media exposure.

Companies worry about becoming entangled in past conflicts.

P.1.3. Loyalty versus integrity

Even though whistleblowing laws protect whistleblowers, many organizations still equate loyalty with conformity, handling issues “quietly” and silence. Whistleblowers violate this unspoken rule. They are often labeled as not a team player, difficult or disruptive.

P.1.4. Whistleblowers challenge power

Whistleblowing often uncovers cultural problems, leadership failures and/or weak governance or incentives. Whistleblowers call out uncomfortable truths and challenge power. Management, however, does not like disruption.

P.2. What can companies do differently?

In many organizations in the recruitment process there is a preference for candidates that are diplomatic, non-confrontational and there is discomfort with candidates who challenge authority.

Organizations should reconsider their hiring practices and assess candidates’ track record of ethical decision making under pressure, the willingness to challenge senior leaders respectfully and the ability to handle conflict.

Organizations should shift their mindset and not view whistleblowers as “trouble” but as employees with a high moral compass.

Q. Investigation

An effective investigation is the linchpin of a whistleblowing framework, serving as the primary mechanism to transform raw allegations into actionable intelligence. Without a forensic, objective, and timely inquiry, even the most courageous disclosure becomes a liability rather than an asset. A robust investigation validates the organization's commitment to integrity, signaling to employees and regulators that "zero tolerance" is an operational reality, not just a marketing slogan. It provides the MLRO and Senior Management with the evidentiary basis required to remediate systemic failures, satisfy statutory reporting obligations, and defend the firm against potential litigation or heavy regulatory fines.

Conversely, a flawed or superficial investigation poses an existential threat to corporate culture and legal standing. If a "payback" motivated claim is not professionally deconstructed, or if a legitimate report is mishandled, the resulting fallout can include the permanent erosion of internal trust and the "weaponization" of the channel by disgruntled stakeholders. The investigation must act as a filter that separates substantiated misconduct from personal grievances, ensuring that disciplinary or corrective actions are legally defensible. Ultimately, the quality of the investigation determines whether a whistleblowing incident results in a strengthened compliance culture or a catastrophic loss of institutional credibility and market confidence.

Q.1. Triage and Investigation Protocols: Ensuring Merit-Based Response

A robust whistleblowing framework is only as good as its triage process. To prevent the Compliance function from being overwhelmed by the "noise" of commercial disputes or HR issues, we implement a tiered assessment approach.

The Triage Workflow

Upon receipt of a disclosure, the Whistleblowing Office (or MLRO) will conduct an initial assessment within [e.g., 7 days] to determine the report's nature:

- **Admissibility Check:** Does the report contain sufficient detail to be investigated? Does it fall under the "Public Interest" or "Regulatory Breach" categories defined in Section E?
- **Conflict of Interest Review:** Ensure no one implicated in the report—or within their direct line of management—is involved in the triage or investigation.

Categorization:

- **Level 1 (Critical):** AML/CTF breaches, systemic fraud, or executive-level misconduct. Immediate escalation to the Audit Committee/Board.
- **Level 2 (Standard):** Operational non-compliance or localized breaches of the Code of Conduct.
- **Level 3 (Misdirected):** Personal grievances or commercial disputes. Redirected to HR or Legal with a formal "Closing Note" to the reporter.

Investigation Principles

Every investigation must be governed by three pillars:

- **Confidentiality:** The identity of the whistleblower is restricted to the "Need to Know" circle.

- **Objectivity:** Investigations are fact-led, not person-led. Evidence is gathered through forensic data review, interviews, and document trails.

- **Promptness:** Investigations should reach a "Preliminary Conclusion" within [e.g., 3 months] to satisfy regulatory expectations under the EU Whistleblowing Directive

Q.2. Investigation

This section acts as the "Standard Operating Procedure" (SOP) within this white paper. It provides a chronological roadmap that ensures every case—whether it's a high-level fraud or a potential "payback" claim—is handled with the same rigorous, defensible methodology.

Q.2.1. Investigation Lifecycle: from Intake to Resolution

To ensure legal defensibility and regulatory compliance, every whistleblowing disclosure must follow a structured six-stage lifecycle. This process ensures that no steps are taken and that the rights of both the reporter and the accused are balanced.

Q.2.1.1 Phase 1: Intake and initial assessment (triage)

The lifecycle begins the moment a disclosure is received via the secure channel.

- **Acknowledge:** Formal receipt sent within 7 days.
- **Triage:** The MLRO assesses if the report meets the "Reasonable Belief" and "Public Interest" criteria.
- **Conflict Check:** Ensure the investigation team is independent of the subjects named in the report.

Q.2.1.2 Phase 2: Scoping and Preservation

Before a single interview is conducted, the investigation must be "boxed in" to prevent data loss.

- **Investigation Plan:** Define the specific questions to be answered and the internal/external resources required (e.g., forensic accountants or external counsel).
- **Legal Hold:** Issue silent instructions to IT to preserve email accounts, server logs, and document versions.
- **Confidentiality Perimeter:** Explicitly define the small circle of individuals who will have access to the file.

Q.2.1.3 Phase 3: Fact-finding and evidence review

This is the "quiet" phase where the heavy lifting of data analysis occurs.

- **Document Review:** Analysis of contracts, transaction logs, and communication threads (the "Paper Trail").
- **Transactional Testing:** If financial crime is suspected, the MLRO conducts a look-back on relevant transactions to identify patterns or anomalies.

- **Corroboration:** Seeking independent evidence that supports or refutes the whistleblower's claims.

Q.2.1.4 Phase 4: the Interview phase

Once the data is understood, the investigation moves to verbal testimony.

- **Whistleblower Interview:** Conducted first to clarify details and identify further evidence (as outlined in Section 5).
- **Witness Interviews:** Speaking to neutral third parties who may have seen or heard relevant events.
- **The "Subject" Interview:** The accused is interviewed last. They are presented with the facts (not the reporter's identity) and given a formal opportunity to respond to the allegations.

Q.2.1.5 Phase 5: Adjudication and Reporting

The investigators move from gathering information to making a determination.

- **Evaluating Evidence:** Testing the facts against the **Balance of Probabilities** (or the relevant legal standard in your jurisdiction).
- **Determining the Verdict:** Is the claim Substantiated, Unsubstantiated, or Vexatious/Malicious?
- **Final Report:** Drafting the Investigation Closing Report for the Board and MLRO (as outlined in Section 7).

Q.2.1.6 Phase 6: Conclusion and Remediation

The final phase focuses on the "aftermath" and organizational growth.

- **Sanctions:** Implementing disciplinary actions for confirmed misconduct.
- **Root Cause Remediation:** Fixing the systemic gap that allowed the breach (as outlined in this whitepaper).
- **Closing Communication:** Notifying the whistleblower that the case is closed and ensuring no retaliation has occurred during the process.

Why this structure is crucial:

- **Consistency:** It proves to regulators that you don't "pick and choose" how to investigate.
- **Fairness:** It protects the rights of the accused by ensuring they have a chance to respond
- **Closure:** It ensures that "payback" claims are formally dismissed and documented as such, protecting the firm from future litigation by the disgruntled party.

Q.3. Evidence preservation and confidentiality

In a whistleblowing investigation, **evidence preservation** and **confidentiality** are not merely best practices; they are the legal safeguards that protect the organization from "spoliation of evidence" claims and the whistleblower from retaliation. For an MLRO, these two pillars ensure that if a case eventually reaches a regulator or a courtroom, the integrity of the process remains unassailable.

Protecting the Integrity of the Truth

The transition from a report received to a formal investigation requires an immediate and disciplined "lockdown" of information. In an era of digital volatility, the window to secure proof is narrow, and the risk of a "leak" can jeopardize both the safety of the reporter and the viability of the defense.

Digital and Physical evidence preservation

The moment a report is deemed "admissible," the Compliance function must trigger a **Legal Hold**. This is particularly critical in cases of suspected financial crime or money laundering, where transaction logs and communications are the primary evidence.

- **Data Minimization & Integrity:** We employ a "Forensic First" approach. Rather than browsing through live files—which can alter metadata—we create mirrored images of relevant drives and communication logs (email, Slack, etc.).
- **Preventing Destruction:** A formal, yet discreet, instruction is issued to the IT and Data departments to suspend all automated deletion protocols for the individuals or departments involved.
- **The Paper Trail:** For physical evidence, a strict **Chain of Custody** is maintained. Every document or device seized must be logged, showing who held it and when, ensuring the evidence remains "admissible" for potential criminal prosecution.

The “Shield of Anonymity” vs “Need to Know”

Confidentiality is the "social contract" between the firm and the whistleblower. If breached, the channel will run dry. However, the organization must distinguish between **Anonymity** (the reporter’s identity is unknown to everyone) and **Confidentiality** (the identity is known to the MLRO but shielded from the rest of the firm).

- **Strict Access Control:** Information regarding the investigation is stored on encrypted, "air-gapped," or restricted-access servers. Only the Lead Investigator and the MLRO have the keys to the whistleblower's identity.
- **The "De-Identified" Reporting Style:** During the investigation, the subject of the report (the "Accused") and witnesses are provided only with the specific facts necessary for them to respond. The identity of the reporter is never revealed unless it is legally mandated by a court or a law enforcement agency.
- **Sanctions for Leaks:** Any employee found to be attempting to "unmask" a whistleblower or leaking details of an ongoing investigation will face immediate disciplinary action, up to and including termination.

Senior Compliance Insight: Effective evidence preservation prevents "payback" seekers from deleting evidence of their own wrongdoing once they realize they are under scrutiny. By securing the data early, we ensure that the facts—and not the narratives—dictate the outcome of the case.

Q.4. Interview stage

The whistleblower interview is perhaps the most delicate phase of the entire process. As a Senior Compliance Officer, your goal is to transition the reporter from a state of potential anxiety (or "payback" motivation) to a state of factual cooperation.

An effective interview is not an interrogation; it is a **forensic information gathering exercise** designed to secure the roadmap for the rest of your investigation.

Q.4.1. The Whistleblower Interview: Eliciting High-Quality Intelligence

The interview serves two purposes: to extract granular detail that the initial report might have missed, and to assess the credibility and "reasonable belief" of the reporter.

Q.4.1.1 Preparation and Environment

- **Neutral Ground:** Conduct the interview in a secure, private location (or via a secure, encrypted video link) where the individual cannot be seen by colleagues.
- **The Two-Person Rule:** Always have two representatives from Compliance—one to lead the questioning and one to take exhaustive contemporaneous notes. This prevents "he-said, she-said" disputes later.
- **No Recording without Consent:** In many European jurisdictions, recording an interview without explicit, documented consent can render the evidence inadmissible.

Q.4.1.2 Dos and Don'ts for the Interviewer

DO	**DON'T**
Manage Expectations: Explain that you cannot provide a "play-by-play" update of the investigation due to confidentiality.	Promise Immunity: Never guarantee that the whistleblower won't face consequences if they are also involved in the wrongdoing.
Use Open-Ended Questions: Start with "How," "Why," and "Describe" to allow the reporter to provide a full narrative.	Lead the Witness: Avoid questions like "So, you saw X stealing the money, right?" Let them provide the details.
Validate the Courage, Not the Fact: Acknowledge the difficulty of coming forward without confirming that you believe their story is "true" before the investigation is done.	Interrogate: Avoid an aggressive tone. If they feel under attack, they may stop providing critical details.
Focus on the "How": Focus on the mechanics of the breach (e.g., "How was the approval process bypassed?") rather than just the "Who."	Show Bias: Even if you suspect a "payback" motive, remain neutral. Facts from a disgruntled person are still facts.

Q.4.1.3 Investigative Questioning Checklist

Use the **TED technique** (Tell me, Explain to me, Describe to me) to ensure maximum information recovery.

I. Establishing the Foundation

- "Describe your role and how you became aware of the information you reported."
- "When did the events occur? Is the conduct ongoing?"
- "Explain the specific policy, law, or internal procedure you believe was breached."

II. Evidence and Witness Mapping

- "Tell me what physical or digital evidence exists (emails, logs, recordings) and where it is currently located."
- "Who else, to your knowledge, is aware of this conduct? Did they participate, or were they also concerned?"
- "Are there any specific documents we should look for that might be hidden or coded?"

III. Assessing Credibility and Risk

- "Have you discussed this with anyone else inside or outside the firm?" (Crucial for assessing "leak" risk).
- "Why did you choose to report this now?" (Helps identify "payback" triggers vs. recent escalations).
- "What do you fear might happen as a result of this report?" (Assesses the need for immediate protective measures).

IV. Closing the Loop

- "Is there anything else you haven't mentioned that might be relevant, even if it seems small?"
- "How can we best contact you securely if we have follow-up questions?"

Q.4.1.4 Red Flags to Watch for

During the interview, the MLRO must look for indicators that the report may be vexatious or malicious:

1. **Inconsistency:** The verbal account differs significantly from the written report without a reasonable explanation.
2. **Focus on Personality over Process:** The reporter spends more time attacking the character of a colleague than describing a breach of regulation.
3. **Withholding Information:** The reporter claims to have "more evidence" but will only release it if they get a specific outcome (e.g., a promotion or the firing of a manager).

Q.4.2. Summary

By following these best practices, the investigation team ensures that the whistleblower feels heard and protected, while simultaneously building an evidentiary file that can withstand the scrutiny of a regulator or a judge.

Q.5. Remediation and Reporting

For a Senior Compliance Officer/MLRO, the goal is to close the loop: informing the governors, satisfying the regulators, and fixing the "why" behind the breach.

Q.5.1. Reporting to the Board and Regulators

An investigation is not truly complete until its findings are communicated to those responsible for oversight and, where legally required, to the state authorities.

Q.5.2. Communicating with the Board of Directors

The Board (or Audit Committee) requires a high-level, objective summary to fulfill their fiduciary duties.

- **The "Executive Summary" Format:** Focus on the **validity** of the claim, the **financial/legal exposure**, and the **adequacy** of internal controls.
- **Anonymity:** Even at the Board level, the identity of the whistleblower should remain confidential unless they are a key witness in a pending legal proceeding.
- **The "No-Action" Report:** If an investigation finds no misconduct, the Board must still be informed to demonstrate that the whistleblowing channel is being actively monitored and taken seriously.

Q.5.3. Regulatory Reporting Obligations

As an MLRO, you must determine if the findings trigger mandatory external reporting (e.g., to the FCA, CSSF, or local FIU).

- **Timeliness:** Many jurisdictions require "prompt" notification of material breaches.
- **Transparency:** Providing a "Self-Disclosure" report can often mitigate the severity of regulatory fines.

Q.5.4. The Investigation Closing Report (Template)

Every formal investigation must culminate in a written **Closing Report**. This document serves as the permanent record of the firm's diligence.

Section	**Content Description**
Case Overview	Summary of the original allegation and the specific regulations/policies involved.

Methodology	List of data sources reviewed, number of interviews conducted, and forensic tools used.
Findings of Fact	A clear statement on whether each allegation was **Substantiated**, **Unsubstantiated**, or **Inconclusive**.
Root Cause Analysis	Identification of *why* the breach happened (e.g., "Culture," "Process," or "Technology").
Recommended Sanctions	Proposed disciplinary actions for the subjects involved.

Q.5.5. Strategic Remediation: Addressing the Root Cause

The final—and most important—step for the Compliance function is to ensure the same issue does not recur. Remediation must look beyond the individual "bad actor" to the systemic failure that allowed the conduct to occur.

Remediation category

1. **Process Remediation:** If the whistleblower revealed a bypass in approvals, the "Four-Eyes" principle must be re-engineered or automated.
2. **Technological Remediation:** Implementing better monitoring software or "Legal Holds" that trigger automatically upon certain risk flags.
3. **Cultural Remediation:** If the root cause was a "tone at the top" issue where managers encouraged rule-breaking for profit, remediation must include mandatory ethics retraining and potentially a review of the firm's incentive/bonus structures.
4. **Control Remediation:** Updating the Risk Register and Internal Audit plan to specifically target the area where the breach occurred.

Q.5.6. Feedback to the Whistleblower

Where possible, and without breaching the privacy of the accused, the whistleblower should be informed that "corrective action has been taken." This reinforces the message that speaking up leads to positive change, deterring future "payback" seekers while encouraging genuine guardians of the firm's integrity.

Figure 2: Whistleblowing Investigation Lifecycle

R. Specifics for the Financial sector

While for example the **EU Whistleblowing Directive** (and similar global standards) provides a baseline for all companies, the financial sector operates in a high intensity "regulatory greenhouse."

The difference lies in the shift from **general ethics** to **mandatory financial stability and crime prevention**.

Below is a thorough analysis of these differences.

R.1. Regulatory Archetype: Discretionary vs. Mandatory

For a regular company, whistleblowing is often framed as a component of "Corporate Social Responsibility" (CSR) or a tool to prevent internal theft. For a licensed financial institution, it is a **statutory pillar of the license itself**.

Feature	**Regular Companies (Non-Regulated)**	**Financial Sector (Regulated)**
Primary Driver	Internal ethics & brand protection.	Financial stability & crime prevention (AML/CTF).
Scope of Reporting	Broad (Health & safety, environmental, HR).	Specific & Technical (Market abuse, capital requirements, AML).
External Reporting	Often a secondary choice for the reporter.	Often a **mandatory** parallel path to the Regulator.
Identity of Oversight	HR or General Counsel.	MLRO, Chief Risk Officer, or Audit Committee.

R.2. The Role of the MLRO: A Unique Accountability

In a regular company, a Compliance Officer manages the whistleblowing process as a neutral investigator. In the financial sector, the **Money Laundering Reporting Officer (MLRO)** has personal, often criminal, liability.

- **Dual Reporting:** In the financial sector, a whistleblower disclosure regarding money laundering doesn't just trigger an internal investigation; it triggers the MLRO's duty to evaluate a **Suspicious Activity Report (SAR)** to the Financial Intelligence Unit (FIU).
- **The "Tipping Off" Conflict:** Licensed firms must navigate the "Anti-Tipping Off" laws. If a whistleblower reports a client for money laundering, the firm must investigate while ensuring the client (the subject) remains unaware—a complexity regular companies rarely face.

R.3. Specificity of "Relevant Wrongdoing"

While regular companies focus on "wrongdoing" in a general sense, licensed firms must monitor for technical breaches that threaten the integrity of the financial system:

- **Market Abuse & Insider Trading:** Specific mechanisms must exist to report manipulation of financial instruments.
- **Prudential Breaches:** Reporting concerns about capital adequacy or liquidity ratios (Basle III / CRD IV).
- **Payment Services Integrity:** Reporting breaches in the PSD2 or Wire Transfer Regulations.

R.4. Direct Channels to the Regulators

Financial regulators (like the **FCA** in the UK, **BaFin** in Germany, or the **GFSC** in Gibraltar) provide dedicated, high-security channels for whistleblowers in licensed firms.

- **"Regulatory Bypass":** Employees in the financial sector are explicitly encouraged by law to go directly to the regulator if they believe the firm's internal "Three Lines of Defense" have failed.
- **Regulatory Assessment:** Regulators use whistleblowing data as a "Risk Indicator." A sudden spike in reports—or a total absence of them—in a licensed firm will trigger a **Thematic Review** or an on-site inspection.

R.5. Higher Standards of Protection & Sanctions

Because the financial sector is systemic, the "Cost of Retaliation" is significantly higher:

- **"Fitness and Propriety":** Retaliating against a whistleblower in a bank can lead to the regulator declaring a CEO "not fit and proper," effectively ending their career in finance globally. In a regular company, the consequences are usually limited to civil employment tribunals.
- **Mandatory Training:** Licensed firms are often required by the regulator to conduct specialized whistleblowing training for all staff, whereas for regular firms, this is often optional or simplified.

R.6. Remediation and systemic risk

In a regular company, remediation might mean firing a corrupt manager. In the financial sector, remediation often requires:

- **Look-back Exercises:** Re-screening thousands of transactions to see if the reported breach was part of a larger systemic failure.
- **Past Business Reviews:** Compensating clients who may have been financially harmed by reported misconduct.

The distinction is clear: In regular business, whistleblowing is about **protecting the company**. In the financial sector, whistleblowing is about **protecting the financial system**. For a licensed firm, failure in the whistleblowing process is not just an HR issue, it is a regulatory failure that puts the firm's "Right to Operate" at risk.

R.7. Regulatory Matrix

This **Regulatory Compliance Matrix** is designed to show the "layering" effect of legislation in the financial sector. While the **General Whistleblowing Directive (EU 2019/1937)** acts as the floor, the

financial sector is subject to several high-ceiling directives that mandate much stricter technical controls and reporting duties.

R.7.1. Regulatory Compliance Matrix: General vs Financial Sector

Area of Regulation	**General Whistleblowing Directive (EU 2019/1937)**	**Financial Sector Specific Regulations (MiFID II, MAR, AMLD, CRD)**
Applicability	All companies with 50+ employees.	Virtually all licensed entities, regardless of size.
Reporting Duty	Reporting is a *right* for the employee.	Reporting is often a *legal obligation* for the firm (e.g., SARs).
Anti-Money Laundering	General reference to reporting financial crime.	**AMLD6:** Specific mandates for reporting suspicious transactions and "tipping off" prohibitions.
Market Integrity	N/A	**MAR (Market Abuse Reg):** Mandatory channels for reporting insider dealing and market manipulation.
Investor Protection	General ethics.	**MiFID II:** Strict requirements for reporting breaches of conduct regarding client assets and advice.
Capital & Stability	N/A	**CRD VI / CRR:** Obligation to report breaches of capital requirements or liquidity risks.
Personal Liability	Limited to civil/employment law.	**Fit & Proper Test:** Directors can be personally barred from the industry for failing to maintain a reporting culture.

R.7.2. Key Financial Sector Differentiators

R.7.2.1.1. The “Lex Specialis” Principle

In European law, when two laws cover the same topic, the more specific law (**Lex Specialis**) takes precedence. For you as an MLRO, this means that while the general Whistleblowing Directive provides the framework for *how* to handle a reporter, the financial regulations (like AMLD6 or MiFID II) dictate *what* must be reported and the *severity* of the consequences.

R.7.2.1.2. Direct-to-Regulator Preference

In the general sector, employees are encouraged to report internally first. In the financial sector, regulators (such as the **EBA** or **ESMA**) explicitly state that whistleblowers have the right to bypass internal channels and go straight to the authorities without needing to "prove" that internal channels failed.

R.7.2.1.3. Proactive Monitoring (The Audit Trail)

Licensed firms must not only have a whistleblowing channel but also be able to prove—via a "Regulatory Audit Trail»that they have actively publicized the channel and trained their staff on its use.

S. Recommendations

Below are several recommendations to regulators and companies to improve Whistleblowing.

S.1. Recommendations to Regulators

S.1.1. Obligation to investigate anonymous allegations

In several EU Member States, anonymous reports can be submitted, but employers or authorities are not legally obliged to investigate or follow up.

Recommendation: in each of the EU member states whistleblowing legislation should require employers to investigate anonymous allegations.

S.1.2. Missing whistleblower protection in Switzerland

In Switzerland there is no protection for whistleblowers in the private sector.

Recommendation: Swiss regulators should adapt local legislation and create whistleblower protection in line with other European countries.

S.1.3. Obligation to set up a whistleblowing system

Except for the regulated sector, there is no obligation in UK for private employers to set up a whistleblowing system.

Recommendation: UK regulators should adapt legislation and require all companies (regulated sector or not) from a certain size to have a mandatory whistleblowing system in place.

S.1.4. Providing Institutional Support to Whistleblowers

Whistleblowers often face extreme stress. To ensure a whistleblower is not "broken" by the process, the State should consider state-funded counseling services.

Recommendation: Authorities should establish a specialized, independent agency (often called a "Whistleblowing Authority" or "Ombudsman") that would provide free, confidential legal and psychological advice to whistleblowers.

S.1.5. Providing financial and career continuity

Whistleblowers can be "starved out" through job loss or blacklisting. Therefore, the State should provide support to whistleblowers.

Recommendation: Authorities must allow for "interim relief," where a court can order an employer to continue paying the whistleblower's salary while a retaliation lawsuit is pending

Recommendation: In some jurisdictions (like the US SEC model), the state provides a percentage of the recovered fine to the whistleblower. This compensates for the high likelihood that the individual may never work in their specific niche industry again due to blacklisting

Recommendation: Governments should penalize "informal" retaliation, such as industry-wide blacklisting, by treating it as a separate criminal offense.

S.1.6. Adapt the scope of NDAs

Companies try to limit whistleblowing /Speak-up by establishing labor contracts and non-disclosure agreements (NDAs).

Recommendation: Authorities must ensure whistleblowers are protected from criminal, civil, and administrative liability (e.g., for defamation, breach of copyright, or trade secret theft) provided they had reasonable grounds to believe the information was true.

Recommendation: Authorities must adopt the law whereby whistleblowing reporting is specifically excluded from private company NDAs.

S.1.7. Government awareness campaigns

Whistleblowing in society is still associated with a negative narrative. Governments have a duty to change that narrative.

Recommendation: Governments should organize educational campaigns whereby whistleblowers are positioned as "Guardians of the Public Interest" rather than "snitches" or "traitors."

Recommendation: Governments should consider establishing awards for ethical bravery to celebrate the positive impact whistleblowers have on the economy and rule of law.

Recommendation: Governments should consider introducing discretionary financial incentive mechanisms, particularly in high-risk areas such as corruption, financial crime, and large-scale regulatory violations. Such mechanisms should be piloted and designed to align whistleblowers incentives with enforcement outcomes, thereby strengthening overall regulatory effectiveness.

S.2. Recommendations to companies

S.2.1. Non-disclosure agreements vs whistleblowing

Companies often use NDAs not to protect confidential information but to bury allegations of misconduct. This practice effectively shields wrongdoers, enabling them to continue their harmful behavior with impunity.

Recommendation: Whistleblowing should be excluded from company NDAs.

S.2.2. Managerial KPIs on psychological safety

Creating a speak-up culture depends on many factors, but certainly creating psychological safety for employees is an important component. In many organizations managers are not held accountable and evaluated on speak-up responsiveness and psychological safety.

Recommendation: Companies should adapt their evaluation and performance system and include KPIs for managers on speak-up responsiveness and psychological safety.

S.2.3. Measuring psychological safety

Psychological safety is very important for employees and a determining factor whether to speak-up. In many organizations the “state of psychological safety” is not being measured.

Recommendation: Companies should conduct regular employee surveys that include specific questions about psychological safety

S.2.4. Adapt the Speak-up to local culture

Organizations roll-out global speak-up programs without considering local cultural factors.

Different organizational cultures require a different emphasis of Speak Up e.g.:

- In hierarchical cultures, it is important to emphasize strong anti-retaliation elements and independence of reporting.
- In global organizations, multilingual and culturally sensitive reporting channels should be promoted
- In high-risk environments, formal reporting channels and anonymity should be promoted.

Recommendation: Companies should adapt Speak-up program to the local culture in the various subsidiaries.

S.2.5. Adapt hiring practice

Whistleblowers are typically people with high integrity and moral values. Challenge senior leaders respectfully should not be seen as problematic, but companies that truly embrace a speak-up culture should welcome such behavior.

Recommendation: Companies should adapt their hiring practices, shift their mindset, embrace whistleblowers as persons with a high moral compass and not view whistleblowers as “trouble”.

S.2.6. Consideration of Financial Incentives in High-Impact Cases

Any consideration of financial incentives should remain discretionary and case-specific, aligned with internal governance frameworks and ethical standards, and subject to appropriate safeguards, including verification of the report’s credibility and impact.

Recommendation: Companies are not expected to implement formal reward schemes for whistleblowing; however, they should not exclude the possibility of financial recognition where a disclosure has clearly generated significant benefit or avoided harm.

S.2.7. Other

S.2.7.1 Robust Triage and Investigation “health checks”

Many organizations have a channel, but few have a high-quality **Triage** process.

- Recommendation: Implement a standardized risk-scoring matrix for incoming reports.
- **Practical Tip:** Distinguish clearly between "Personal Grievances" (HR matters) and "Public Interest Disclosures" (Whistleblowing) at the point of entry. Provide a "Feedback Loop" protocol that ensures the whistleblower is updated within the statutory 3-month window (under the EU Directive), even if the investigation is ongoing.

S.2.7.2 Protecting the "Facilitator "and Third Parties

Modern regulations (and the EU Directive specifically) have expanded protection beyond just the whistleblower.

- Recommendation**:** Explicitly extend anti-retaliation protections to "Facilitators"—colleagues or relatives who assist the whistleblower.
- **Practical Tip:** Update your Whistleblowing Policy to state that any retaliation against a person who *helped* gather evidence is treated as a disciplinary offence, equal to retaliating against the whistleblower themselves.

S.2.7.3 Integration with ESG and EU AI Act

As of 2026, whistleblowing is a primary tool for detecting "Greenwashing" and AI-related risks.

- Recommendation**:** Ensure your whistleblowing channel is explicitly listed as a reporting mechanism for breaches of the **EU AI Act** and **Corporate Sustainability Reporting Directive (CSRD)**.
- **Practical Tip:** Train your intake team to recognise "Algorithm Bias" or "Environmental Misrepresentation" as high-priority disclosures, as these now carry significant specialized regulatory penalties.

S.2.7.4 Integration with the broader compliance management system

Whistleblowing should not be a standalone tool but should be integrated in the broader compliance management system and culture.

Recommendation**:** Whistleblowing/Speak-up must be integrated in the broader compliance management and should be an integral part of the lifecycle management approach "prevent-detect-investigate" where whistleblowing interacts with the other components.

S.2.7.5 "Speak-up" Training for Middle Management

The biggest failure point in whistleblowing is the "First Responder"—the line manager who receives an informal complaint and inadvertently shuts it down.

- Recommendation: Move training away from "how to use the portal" for employees, toward "how to listen" for managers.
- **Practical Tip:** Conduct "Micro-Simulations" for middle managers where they practice reacting to a sensitive disclosure without showing defensiveness or asking, "Why didn't you come to me sooner?"

S.2.7.6 Data Privacy "Siloing" (GDPR vs The right to Know)

There is a constant tension between the whistleblower's anonymity and the "Accused's" right to know the allegations against them.

- Recommendation: Establish a "Data Minimization" protocol for investigation reports.
- **Practical Tip:** Ensure the investigation file is "Siloed" from the general HR file. If the accused person makes a Subject Access Request (SAR), the whistleblower's identifying details must be redacted or held in a separate, highly restricted digital vault to prevent "accidental" unmasking.

S.2.7.7 Measuring Effectiveness through "Silence Mapping"

Compliance Officers often think a "zero-report" department is a "clean" department. It usually isn't.

- Recommendation: Use "Silence Mapping"—comparing employee engagement survey results against whistleblowing data.
- **Practical Tip:** If a high-risk department (e.g., Procurement or Sales) has had zero reports for two years but shows "low trust" in engagement surveys, recommend a targeted "Culture Audit" rather than assuming no news is good news.

Suggested Structure

Recommendation	**Objective**	**Key Action**
Active Triage	Prevent "Grievance Clog"	Use a 48-hour risk-rating system for all new reports.
Facilitator Shield	Prevent "Secondary Retaliation"	Update policies to protect those who assist the reporter.
Managerial Response	Eradicate the "Chilling Effect"	Mandatory "Active Listening" training for all Level 1 managers.
ESG/AI Alignment	Future-Proofing	Explicitly include AI ethics and Greenwashing in the scope.
Root Cause Analysis	Continuous Improvement	Report *themes* (not just numbers) to the Board quarterly.

T. Interview with Pav Gill

interview with Pav Gill – 22nd April 2026

Pav Gill (PG) is a Singaporean lawyer and entrepreneur, best known as the whistleblower who exposed the Wirecard scandal, one of the largest corporate frauds in European history.

Early Life and Education

Born and raised in Singapore, Gill was raised by a single mother in subsidised housing. He studied law at the National University of Singapore, graduating in 2008.

Career and the Wirecard Scandal

After beginning his legal career at prestigious 'Magic Circle' firms—including Allen & Overy and Clifford Chance—Gill transitioned into the fintech sector. In 2017, he was appointed as the first in-house Head of Legal for the Asia-Pacific region at Wirecard, a German payment processor then valued at billions of euros.

While based in Singapore, Gill discovered evidence of widespread financial misconduct and accounting fraud. Despite facing intense internal pressure and personal risk, he ultimately provided crucial documents to the *Financial Times and Suddeutsche Zeitung*. His revelations led to the company's collapse in 2020 after it admitted that €1.9 billion in cash likely did not exist.

Recent Ventures and Recognition

Following the scandal, Gill founded **Confide**, a compliance workflow and case management software platform designed to help organizations detect and manage internal risks securely. His story has been featured in several documentaries, including Sky Studios' *Wirecard: A Billion Euro Lie*.

For his bravery and commitment to ethics, he has received numerous accolades, such as the **ACFE Cliff Robertson Sentinel Award** and the **Blueprint for Free Speech Special Recognition Award**. He is now a prominent keynote speaker on corporate governance and integrity.

The interview was conducted by Patrick Wellens (PW) and Carlos M Martins (CM) in representation of ENFCO (The European Network for Compliance Officers) on the 22nd April 2026.

CM & PW: First of all, we would like to thank you for your availability to speak with us and to allow us to publish this interview as the foreword of our ENFCO Whitepaper on Whistleblowing.

PG: It is a pleasure participating in your project.

CM: To start with, could you please kindly provide us with more background on you and your history?

PG: It is a long story, so let me break it into a few parts:

Discovery of the Fraud

"I joined Wirecard as Head of Legal for Asia-Pacific, covering 13 markets. Very quickly, things stopped making sense. Most of our Asia-Pacific entities were loss-making, yet the group was still reporting earnings in the hundreds of millions, broadly in line with Europe.

From a fintech perspective, the revenue was hard to see. We marketed ourselves as a high-end technology company, yet competitors like Alipay were far more sophisticated. Wirecard were far more 'fin' than 'tech.' That branding also helped it avoid the level of scrutiny a traditional financial institution would have faced."

The Whistleblower and the Investigation

"The turning point came when a whistleblower from the finance team approached me. She was frightened and wanted to distance herself from transactions she believed were illegal. I met her at a café near the office to protect her identity. I called her 'Bobby' and I have never disclosed who she was.

I reported the matter to the Deputy General Counsel in Munich and was told to start an investigation. After I got access to about 85GB of inbox data from the main suspects, I brought in an external law firm in Singapore because I wanted an independent third-party view. The preliminary report identified several potential offences and recommended a full investigation. Instead, the company used it as a gap analysis to see where it was exposed. At that point, I had become the problem."

Retaliation and Personal Risk

"The retaliation was serious. They tried to frame me with a fake HR case. When that failed after three months, the next move was to get me onto what looked very much like a one-way business trip to Jakarta.

The plan was being driven by Edo Kurniawan, the prime suspect in the investigation. He was later promoted in the middle of it all with a group-wide email, which tells you a lot about the culture. When I first met him, he told me he was married to a drug-dealing family in Jakarta. When he insisted I travel there and said I would be well taken care of, I understood the message.

While I was pushing back on the trip, I received two anonymous calls on my landline from Germany. The message was simple: 'Pav, we understand you are being made to go to Jakarta. Do not go. You will not come back.' I refused to go. That then gave Wirecard the business reason it wanted to force my resignation.

Even after I left, the pressure continued. My mother and I found ourselves being followed by dubious-looking individuals. Wirecard also set up fake job interviews with 'friendly' companies to see whether I would say something negative about the company and give them a pretext to sue me. They wanted to make life as difficult as possible."

Going Public

"Eventually my mother had had enough. She reached out to the Financial Times and I began working with its journalists in secret. When the FT published, the first reaction in Germany was to go after the newspaper rather than the company.

The stress took a heavy toll. My mother, who neither smoked nor drank, suffered a stroke and was then diagnosed with stage-two lung cancer, which led to half her lung being removed. That only hardened my resolve. After eighteen months of pressure from multiple directions, Wirecard finally collapsed."

A year later, when the Sky documentary Wirecard: A Billion Euro Lie was released, I decided to go public. My mother and I were in the film, so the secret was not going to hold much longer anyway."

The Birth of Confide

"Since becoming known as the whistleblower, I have spoken at a number of events and watched the EU Whistleblowing Directive roll out at the same time. I kept asking myself what the larger purpose of the whole experience had been. Most companies like to talk about hotlines and intake. What is usually missing is the part that comes after.

That is what led me to found Confide. The real weaknesses tend to be who sees the report, how it is investigated, whether there is an audit trail and whether anything is resolved. Confide was built to address that. We provide an end-to-end whistleblowing and case management platform, together with training for case managers in HR, Legal and Internal Audit. My aim was to turn a hard experience into something useful for the next person."

CM: What a story! Following from your story, would you say that if a whistleblower goes public, they run the risk of being blacklisted and scare off companies, and therefore make it very difficult for them to find employment?

PG: What worries many employers is the fact that the employee went outside the organization. Many still see these matters as internal. Once someone goes to a regulator, the press or an outside lawyer, that person is often viewed as a red flag. That is where the idea of 'once a whistleblower, always a whistleblower' comes from.

There are exceptions. A regulated firm or a company that is serious about governance may see that background as a strength. They may want a lawyer, compliance officer or auditor who has lived through a major failure and knows where the red lines are.

That said, the ideal case is still the minority. In practice, many companies remain wary because they fear the issue will leave the building.

PW: "I've been thinking quite a bit about how we can change the prevailing perception of whistleblowers. We need to move away from the idea that these individuals simply have a 'propensity to go external' and instead recognize them as people with exceptionally high integrity and ethical standards.

In the modern corporate world, every organization talks about the importance of ethics, integrity, and codes of conduct. If those values are truly a priority, then a whistleblower is exactly the kind of person you would want in your company. Yet, the reality remains that they are often viewed with suspicion. I am interested in how we can bridge that gap and shift the narrative so that these individuals are seen as assets rather than liabilities."

"How can we shift the corporate perception of whistleblowers, so they are valued as champions of high integrity rather than being viewed as risks to the organization's internal privacy?"

PG: "I do not think perception changes in the abstract. People bring their own views and biases. These situations have to be judged case by case. Someone who speaks up about sexual harassment and helps drive real change is often seen very differently from someone who was involved in the wrongdoing or is trying to leverage the situation for money.

Motives will always be examined. That is why sweeping statements about whistleblowers do not help.

Part of the problem is that the term 'whistleblowing' is now used far too broadly. Sometimes the person is not exposing a criminal scheme at all. They are raising an operational risk, a control failure or something that simply does not add up. We will see more of that in AI as well, whether it is unethical code, back doors into customer data or a conflicted vendor pushing a bad product.

I think of it as a hierarchy of reporting:

1. Whistleblowing: systemic, serious or potentially criminal issues.
2. Grievances: personal or workplace complaints.
3. Disclosures: raising a concern that may not be misconduct but still needs attention.

Companies need environments where people can ask questions or raise concerns without immediately being treated as adversarial. Spotting a discrepancy in an invoice does not mean the company is fraudulent. It may be a mistake. The issue is whether people feel safe enough to raise it.

That is why employability and reputation always come back to facts, context and how the next employer reads the situation."

CM: "During the preparation of our paper, we had a heated debate regarding **whistleblower incentives**. On one side, you have the US model—and more recently the UK—which has taken the stance that if a whistleblower comes forward and a case is proven, they deserve financial compensation. On the other side, Europe operates primarily on a **protection-based model**, focusing on legal safeguards rather than financial rewards.

Looking back at your own journey as a whistleblower, would the presence or absence of a financial reward have influenced your decision to come forward? Is whistleblowing purely a matter of conscience that happens independently of incentives, or do these rewards play a functional role in the decision-making process? How do you view that dynamic?"

The precise question is: “"In your experience, is whistleblowing driven entirely by an individual's conscience, or are financial incentives a necessary tool to offset the life-altering professional and personal risks involved?"

PG: "I am generally wary of legal structures that pull people straight out of the company and into the hands of the authorities. The US model creates a strong pull factor through financial incentives. Other systems have the opposite problem and make internal reporting almost pointless.

Take Malaysia. If the first person you speak to is not an enforcement agency, you can lose protection. I do not like that approach. Companies should have the chance to address an issue internally first, provided the internal channel is safe and credible.

That takes you back to first principles: is the report anonymous, is there real protection of anti-retaliation and does the company actually walk the talk?

Most whistleblowers are trying to discharge a burden. They see something that does not make sense and want to report it so it can be dealt with. The problem begins when the company turns the reporter into the issue. That is when people start looking outside.

Financial reward is not the core driver in my view. A reward may make sense in certain public-interest cases, especially where public funds are involved, but whistleblowing should not be built around payout culture."

PW: "We have discussed this briefly, but it is clear that many European companies are desperate for their employees to report issues internally first. In your experience, what is the single biggest factor that causes a whistleblower to lose faith in their company’s internal reporting channels? What is it that ultimately compels them to go outside—whether to a regulator or to the press?"

PG: "It usually comes down to two things. First, can the person trust the channel? If the system sits on the company’s own network and IT can work out who filed the report, anonymity is already compromised.

Second, does the company do anything once a report comes in? Outcome matters. When people see that a report led to a real investigation and a real sanction, even against someone senior, they start to trust the process.

So the answer is safety first, then execution. If either is missing, people lose faith very quickly."

CM: "We previously discussed the financial rewards linked to whistleblowing, but there is a growing concern regarding malicious reporting. Critics of the incentive model argue that high financial rewards might encourage 'bounty hunting'—where individuals report non-existent cases or fabricate evidence simply to claim a payout. Within the whistleblower community, how valid is the concern that financial incentives lead to a surge in fraudulent or bad-faith reports?"

Essentially: "Does the implementation of financial rewards for whistleblowers create a significant risk of 'bounty hunting,' where the desire for a payout leads to malicious or fabricated reporting?"

PG: "The fear of malicious reporting is usually overstated. A report is only as strong as the evidence behind it, so weak or bad-faith allegations are often easy to filter early.

From the company's perspective, more information is usually better than less. Something that looks minor today may become important later when you see the broader pattern. The real challenge is not volume. It is handling.

At Confide, we separate grievances from whistleblowing product-wise for exactly that reason. Someone complaining about the end of remote work or lashing out after dismissal is not necessarily a whistleblower. A structured system helps you sort that properly and document why a case was closed if the evidence never materialises.

Knowledge is power. Even a troubled company is better off finding out internally and acting than being surprised by a dawn raid or its own obituary in the press."

CM: "You've raised a critical point regarding timing. Consider an employee who has been with a company for 20 years with no apparent issues. The moment they are dismissed, they suddenly file a claim for sexual harassment or bullying.

As an investigator, how do you differentiate between someone who is simply lashing out in retaliation for their dismissal and someone who has a genuine grievance they were too terrified to report while their livelihood was at stake? Once they have 'lost everything,' they may feel they finally have nothing left to lose by speaking out.

From the company's perspective, drawing that line is incredibly difficult. You want to take every case seriously, but often it can look like a bitter reaction from a disgruntled ex-employee. It's a complex grey zone. How do you navigate that?"

PG: "These cases have to be assessed one by one, though analytics can help. If there is a wave of reports after a redundancy round, that is relevant context. It is not a reason to ignore the reports.

You have to go back to first principles. Can the allegation be substantiated? It is also critical to separate performance from conduct. Someone may be lawfully dismissed for poor performance and still have a legitimate complaint about harassment or abuse by a manager.

That misconduct is a separate organizational risk. If a senior person has a propensity for that behavior, the board needs to know. It goes to culture, reporting lines and the broader control environment.

So, the task is not to pick one story and discard the other. It is to investigate both properly and understand what risk the company is actually carrying."

The Dual-Track Investigation Model

To manage the "grey zone" of post-termination reports, companies should adopt a dual-track approach to ensure both legal compliance and ethical integrity.

- **Track 1: The Performance Case:** Was the termination or redundancy based on objective, documented business needs or performance metrics? If yes, the company's legal position regarding the dismissal remains intact.
- **Track 2: The Conduct Case:** Regardless of the employee's performance, did the alleged misconduct occur? This investigation focuses on the accused party and the company's culture.
- **The Intersection:** Investigators must determine if there is a causal link—i.e., was the "poor performance" actually a result of the employee rebuffing the manager's advances?"

PW & CM: "Whistleblowing often has a catastrophic emotional and financial impact. When individuals decide whether to speak up, they are forced to weigh their integrity against the risk of bankruptcy, losing their homes, or being blacklisted from their industry for a decade or more.

We've been considering the concept of full remediation rather than 'bounty hunting.' The goal wouldn't be to make the whistleblower rich, but to ensure they are made whole. Could we introduce a state-mandated mechanism, perhaps a Whistleblower Compensation Fund—to cover legal fees and lost future earnings?

This could be structured similarly to investor or client protection schemes in the banking sector. All licensed firms would contribute a levy to a central fund. If a whistleblower suffers damages due to retaliation or job loss, this fund would compensate them for their actual losses. What are your thoughts on such a model, and do you think an insurance-based or fund-based structure is the best way to prevent whistleblowers from falling into financial ruin?"

So, the real question would be: ""Should the state implement an industry-funded 'Whistleblower Remediation Fund'—modelled after investor protection schemes—to ensure that individuals who expose wrongdoing are compensated for their actual legal fees and lost earnings rather than being incentivised by speculative bounties?"

PG: "I am cautious about adding broad new financial burdens on companies. The practical problem with most compensation models is that they usually assume the whistleblower has identified themselves. You cannot reimburse someone or compensate them if you do not know who they are.

That takes you straight into questions of quantum, proof and years of litigation. Once you widen it beyond legal fees, the model becomes very hard to administer fairly.

A narrower legal-fees model is easier to defend. If a whistleblower gets legal advice and a credible claim of retaliation is established, there may be a case for a central fund to reimburse the legal work. That is far simpler than speculative payout models tied to recovery. If you base compensation on recovered funds, what happens when there is no recovery even though the retaliation was real? You create another layer of dispute.

My view is that the more urgent job is to audit and enforce company processes properly. The EU Directive was a good start, but enforcement is uneven. Spain can impose fines up to €1 million. Germany's maximum fine is €50,000. For a large company, that is not a meaningful deterrent. Until the stick is real, the framework will remain too easy to ignore."

CM: "In the Wirecard case, you eventually became the public face of the investigation. However, most people want to avoid that level of exposure and remain entirely anonymous.

What advice would you give to someone who wants to report wrongdoing while staying under the radar? It often feels like companies are actively trying to 'unmask' whistleblowers, while the individuals themselves—rightly concerned for the safety of their families and their careers—are desperate for protection.

The technical challenge is significant. Many whistleblowers are not 'tech-savvy' and may not realize that logging in from a company computer or even a home network can reveal an IP address. Even with basic masking, a determined hacker or a sophisticated corporate IT team might still find a way to trace the initial login. In an environment where the company may be actively working against you, how do you truly ensure your anonymity remains ironclad?"

The question would therefore be: "Given that most whistleblowers lack advanced technical expertise, how can they trust that a reporting system is truly anonymous, and what are the essential 'digital hygiene' steps they must take to ensure their identity isn't exposed by a determined corporate IT department?"

PG: "Technical anonymity has limits. If only two or three people know a set of facts, the company may work out who reported it regardless of how strong the encryption is.

That is why I tell whistleblowers to build a careful chronology. Record when you reported, who had access to the issue and what changed afterward. In the EU, where the burden of proof has shifted in retaliation cases, that timeline can be very powerful.

I often say Wirecard was a rare case of 'successful' whistleblowing because the company actually collapsed. Even then, I stayed anonymous for a year after the crash because an insolvent company can still sue you.

In most cases, I tell people to work backwards from the outcome they want before they do anything.

- Do you want to expose the company publicly?
- Do you want compensation for dismissal or retaliation?
- Do you want to trigger regulatory action?
- Or do you simply want to discharge the burden, sleep at night and move on?

Once you know the 'why', you can build a strategy around it and reduce avoidable risk."

CM: "If I were looking for a new job today and wanted to assess a company’s integrity, what should I look for in their whistleblowing policies and procedures? Are there specific red flags that would signal a poor reporting culture or a lack of protection? If I’m reviewing their internal documents during the hiring process, what are the warning signs that should make me think twice about choosing that employer?"

PG: "I am deeply skeptical of the traditional hotline or outsourced call-center model. More than 95% of the people who contact me on LinkedIn are senior employees: CFOs, managing directors, heads of department. They are not going to discuss a serious fraud with a random third-party call handler who does not understand the business.

The model also creates obvious risks:

- Translation risk: sensitive information may be pushed to third-party translators who should never see the case.
- Routing risk: we have already seen cases where reports were sent straight back to the people being accused.

I am equally wary of companies that have nothing more than a policy document and a shared email address. In those setups, you do not know who is behind the screen or who can access the data.

If I were assessing an employer, I would focus on two things:

1. Independent oversight: the case managers should report at a level that can hold management to account, ideally through the audit and risk structure or the board.
2. Secure infrastructure: the company should have a dedicated platform rather than a paper policy and a hope that nobody misuses the inbox."

PW: "To follow up on that, would a company's **annual transparency report** increase your confidence in their system? For example, if a firm publicly disclosed the number of whistleblowing cases they received, the number of investigations conducted, and the resulting disciplinary actions—such as the number of employees or executives fired—would that serve as a credible indicator of a healthy reporting culture?"

PG: "We have to be honest about how the world works. Most people need a job to survive. They need the pay cheque.

During a hiring process, very few candidates are conducting a forensic review of who got fired for whistleblowing or how prior cases were handled. Many will rationalize the risk and tell themselves they can fix the problem from the inside. That is human nature. The need for employment is usually stronger than the red flags."

CM: "Nowadays, AI is the central topic of conversation. Do you believe AI will make it easier or more difficult for whistleblowers to report wrongdoing? On one hand, people might be scared off by the feeling that AI systems can 'unmask' them even faster than humans ever could. On the other hand, it could streamline the reporting process.

How do you view this shift? Is AI an advantage or a disadvantage for transparency, and what is your feeling on its impact on anonymity?"

Or asked differently: "As AI becomes more sophisticated at pattern recognition, will it ultimately serve as a 'digital panopticon' that makes true anonymity impossible, or can it be engineered as a 'shield' that protects whistleblowers by scrubbing their reports of identifying data?"

PG: "AI can help or hurt. It depends entirely on how it is deployed and governed.

If the system is ring-fenced, transparent and not exposing data to third parties, AI can improve the front end. An AI interface may be better than an outsourced call center because it does not judge the reporter. It can capture the basics and flag urgent cases, such as self-harm or possible criminal activity. It should not be giving legal advice.

The first reporting stage is where many people drop off because the process is too long or too clumsy. AI can help through conditional logic. For example, if someone in construction or healthcare reports an injury, the system can immediately ask the right follow-up questions while the reporter is still engaged.

It also has a role on the backend in producing reports for boards, auditors and regulators, and in helping organizations meet feedback obligations under the EU Directive. The key is disclosure. People need to know how AI is being used and where its role stops."

PW: "Whistleblowing is often described as a 'lonely path.' Suddenly, you find yourself fighting a massive corporation entirely on your own. While you may have the support of close family members, the psychological weight of the battle can be devastating to your mental health, your sanity, and your physical well-being.

In your opinion, what should companies be doing to provide psychological safety nets during the investigation? How can an organization support and assist a whistleblower throughout the process to ensure they aren't crushed by the experience? How can companies move beyond legal compliance to provide real, human support?"

PG: "I am not a psychologist, so I would not pretend to solve the culture piece in a neat slogan. In practice, a safety net depends on two things: the whistleblower has identified themselves and the company actually wants to act in good faith.

Once a real investigation is underway, there are practical protections available. That may mean gardening leave, moving the person out of a hostile reporting line or creating some other safe environment while the investigation runs.

But the most important discipline is simpler than that. When a report arrives, the first question should never be, 'Who is this person and why are they saying this?' If you start there, you are already moving away from the facts.

The better question is: even if this came from an alien, is it true, and would ignoring it harm the company? If the answer is yes, act on the substance first. Motive and identity can wait."

CM: "Some boards today still hold the antiquated view that whistleblowers are simply disloyal employees or 'troublemakers' who don't deserve the attention they receive. They see a report as a personal attack on the company rather than a tool for governance.

If you were confronted with a board that held these views, what advice would you give them to help them realize they are getting it wrong? Given that the 'tone from the top' is the single most important factor in a company's culture, how do you convince a skeptical board that embracing whistleblowing is actually in their best interest?"

PG: "From a governance perspective, boards are the ones on the line when things go wrong. Their basic question should always be: 'What did we do to prevent this?'

A lot of resistance comes from the view that most reports are malicious or merely employee grievances. Even if that were true, it is not a reason to dismiss the channel. A board that sees whistleblowing as an inconvenience is itself a red flag.

Technology helps, but tips still matter. The ACFE has found that 43% of occupational fraud is detected through tips. That is a huge part of the risk picture.

If a board cannot understand that, then perhaps the board itself is part of the governance problem."

PW: "As we look at the landscape in 2026, it appears that the legal environment is finally beginning to catch up with the reality of whistleblowing. With these positive shifts in legislation and corporate accountability, what is the one thing you hope the next generation of employees will never have to experience? Given the progress we've made, what part of your own journey do you hope becomes a relic of the past?"

Or asked differently: "If the legal landscape of 2026 has finally matured, will the next generation of employees be able to report misconduct as a 'standard business procedure' rather than a 'life-altering act of bravery'?"

PG: "This generation has more access to information than any generation before it and far more ways to distribute it. You can see that in the way people use Reddit, X and Google Reviews to expose bad conduct. Tolerance for misconduct is lower now, and that is good for society.

But I would still give one strong warning: do not start downloading gigabytes of company data and taking it home just because you think you are right.

There is a real difference between having the truth on your side and having the resources to fight a company in court. If you mishandle data, the company may sue you for theft before the underlying misconduct is ever tested."

CM: "If you have discovered information that proves your case, you face a terrifying choice. If you download that data to a USB drive or email it to your personal account, you are likely in breach of your employment contract and data protection laws. However, if you wait, you risk the company identifying you as the whistleblower and cutting off your access before you can secure the evidence.

Is there safe middle ground? For instance, if you forward that data to a lawyer specifically to seek legal advice, does that provide a layer of protection? Or are you still in 'muddled waters' legally the moment that data leaves the company's-controlled environment?"

PG: "The first step is to get legal advice before you do anything. In a highly regulated environment, unauthorized data transfers can end your career immediately.

In many cases, you do not need nearly as much data as you think. A safer approach is to record where the information sits so that a regulator, law-enforcement agency or the company itself can secure it properly once the matter is reported.

If you do need to preserve evidence yourself, your position is far stronger if you can show it was done solely to support a legitimate whistleblowing case and not for personal gain or to benefit a competitor.

Every case is different. The point is to avoid exposing misconduct by committing a separate breach on the way there."

CM: "As a final question—and with our sincere thanks for your time—I'd like to look back at your own experience with Wirecard. Given everything you know now, the insights you've gained, and the personal and professional toll of that journey, is there anything you would have done differently if you were starting over today? If so, what would that be, and how would it have changed the outcome for you?"

PG: "Honestly, I do not think I would have done much differently. Once it started moving, the situation took on a life of its own. Looking back, I am not sure any realistic change on my part would have materially altered the outcome."

PW & CM: Pav, it was great to have the opportunity to speak with you. We would like to thank you for the hour we were allowed to share with you and ask as much as we wanted. Thank you for your openness and for your frank answers. Our readers will appreciate all those invaluable insights you have provided us and them. A big thank you on behalf of ENFCO.

U. Disclaimer

1. General Information and Purpose: This strategic paper, “The ENFCO Whistleblowing Framework: navigating challenges, protections and best practices," (the "Paper") has been prepared by the European Network for Compliance Officers (ENFCO) for informational and discussion purposes only. It aims to stimulate dialogue, share perspectives, and contribute to the ongoing development of compliance practices within Europe and beyond. The views and opinions expressed herein are those of the authors and do not necessarily reflect the official policy or position of any organization, institution, or legal authority unless explicitly stated.

2. Not Legal Advice: The content of this Paper is not intended to constitute, and should not be relied upon as legal, professional, financial, or any other form of advice. It is a strategic and conceptual document and does not address the specific circumstances of any individual, entity, or legal jurisdiction. Readers should consult with qualified legal and compliance professionals for advice pertaining to their specific situations and before making any decisions or taking any actions based on the information presented in this Paper.

3. Accuracy and Completeness of Information: While ENFCO has made every effort to ensure the accuracy and completeness of the information presented in this Paper as of the date of publication, we do not guarantee the same. The field of compliance, as well as relevant legal and regulatory frameworks, is dynamic and subject to continuous change. ENFCO and the authors disclaim all liability for any errors or omissions, or for the results obtained from the use of this information.

4. Forward-Looking Statements: This Paper may contain forward-looking statements or projections regarding future trends, developments, or outcomes in the field of compliance. These statements are based on the authors' current expectations and assumptions and involve known and unknown risks, uncertainties, and other factors that may cause actual results, performance, or achievements to differ materially from those expressed or implied by such forward-looking statements. ENFCO undertakes no obligation to update or revise any forward-looking statements to reflect new information, events, or circumstances.

5. Limitation of Liability: To the fullest extent permitted by law, ENFCO, its members, directors, officers, employees, agents, and the authors of this Paper shall not be liable for any direct, indirect, incidental, consequential, special, punitive, or exemplary damages, including but not limited to, damages for loss of profits, goodwill, use, data, or other intangible losses (even if ENFCO has been advised of the possibility of such damages), resulting from: (i) the use or the inability to use the Paper; (ii) any content or information contained in the Paper; (iii) any reliance placed on the completeness, accuracy, or existence of any advertising, products, or other materials appearing in the Paper; or (iv) any other matter relating to the Paper.

6. Intellectual Property: This Paper, including all its content, is the intellectual property of ENFCO and/or the contributing authors and is protected by copyright and other intellectual property laws. Reproduction, distribution, modification, or transmission of any part of this Paper without the prior written consent of ENFCO is strictly prohibited, except for personal, non-commercial use, provided that all copyright and proprietary notices are retained.

V. Acknowledgment

We gratefully acknowledge the invaluable contributions of the following individuals, whose expertise, insights, and collaboration significantly enriched this white paper:

- **Andrijana Bergant**, President, EICE- European Institute for Compliance and Ethics, Slovenia
- **Barbara Dircksens,** General Manager**,** ASCOM - Asociación Española de Compliance
- **Carlos Martins**, Chairperson, Gibraltar Association of Compliance Officers
- **Diego Rechaca Plo**, Board member ASCOM - Asociación Española de Compliance
- **Jerica Jančar,** Board Member**,** EICE- European Institute for Compliance and Ethics, Slovenia
- **Radomir Dukov**, Chairperson, Bulgarian Association of Anti-Financial Crime Experts
- **Patrick Wellens**, Chairman, Ethics & Compliance Switzerland and Chief Compliance Officer Association of Corporate Investigators

Their diverse perspectives and dedication to advancing “The ENFCO Whistleblowing Framework: navigating challenges, protections and best practices” were critical to the quality and depth of this publication.

We also extend our thanks to the broader community of professionals and stakeholders who supported this initiative through feedback, dialogue, and peer review.