Researching And Discovering Potential Whistleblowers

By Lekhana Molleti (darivxe)

Contents

1. *Executive Summary*

This report examines potential whistleblowers identified through open-source intelligence gathered from the surface web, deep web, and dark web. Three cases showed strong indicators of credible whistleblowing intent: Dr Christopher Day's disclosures about safety failures inside the NHS, Aaruni Abhishek's reporting of a privacy and security breach at TD Bank, and an anonymous compliance professional linked to exposing fraud involving Ho Wan Kwok (Miles Guo).

Each case was cross-verified with external evidence including tribunal records, regulatory filings, news articles, and legal documents. The individuals demonstrated clear personal impact, direct exposure to organizational misconduct, and behaviour consistent with early-stage or active whistleblowing.

The findings show a repeatable pattern: organizational failures, retaliation or risk to the individual, and eventual movement toward external reporting. This report outlines these patterns and assesses the likelihood of each individual's whistleblowing activity based on OSINT-derived evidence.

1.1 *Scope*

The scope of this investigation is limited to the identification, analysis, and classification of potential whistleblowers using OSINT methods.
This includes:

Identification of individuals
Individuals showing signs of whistleblowing intent across Reddit, LinkedIn, Tor forums, and other online platforms were reviewed. Only cases with verifiable external evidence were included in detailed analysis.

Organizational-level verification
Public records, legal filings, tribunal decisions, news coverage, and regulatory documents

were examined to confirm whether the organizations associated with the individuals were involved in misconduct, breaches, or fraud.

Behavioural assessment
Indicators such as attempts to contact journalists, anonymous posts about secure communication, and disclosure of internal events were evaluated to determine whistleblowing likelihood.

Exclusions
This report does not perform doxxing, deanonymization, or invasive investigative techniques.
Suspected whistleblowers who lacked verifiable supporting information were excluded from outcome sections, though early-stage behavioural indicators were discussed separately.

1.2 *Methodology*

A structured OSINT methodology was used to ensure accuracy, repeatability, and evidence-based conclusions. The process followed four stages:

1. Collection

Information was gathered from:

- Reddit communities including r/Whistleblowers, r/onions, and related forums
- Tor Browser support forums and onion-space discussions
- LinkedIn posts, articles, and personal statements
- News outlets, regulatory filings, tribunal records, and press releases
- Verified legal documents and publicly accessible databases

Search queries, advanced operators, and platform-specific filters were used to uncover relevant discussions and public disclosures.

2. Verification

Each claim made by an individual was cross-checked with:

- Legal filings (tribunal evidence for Chris Day, CHRC filings for Aaruni, SDNY indictments for Miles Guo)
- News reports covering organizational misconduct
- Regulatory or government-issued documents
- Multi-source corroboration to reduce reliance on a single viewpoint

Only cases with confirmed organizational issues were elevated to full analysis.

3. Analysis

Collected data was reviewed to identify:

- Patterns of internal misconduct
- The individual's relationship to the events
- Indications of retaliation, suppression, or negligence
- Behavioural signs of whistleblowing intent
- The escalation pathway from internal reporting to external disclosure

This step also involved classifying anonymous actors based on online behaviour, phrasing, and context.

4. Assessment & Classification

Individuals were classified as potential whistleblowers when they demonstrated:

- Credible knowledge of internal wrongdoing
- Personal impact or harm resulting from the misconduct
- Evidence of seeking outside channels for disclosure
- Alignment with known whistleblower behavioural models

The methodology remains fully OSINT-compliant and avoids unethical or intrusive practices.

1.3 *Working Hypothesis*

This investigation was guided by a set of hypotheses developed from behavioural indicators, historical whistleblower cases, and patterns observed across social media, news reports, and dark-web forums.

H1 — Early-stage whistleblowers seek secure communication channels.
Individuals asking about VPNs, Tor, Tails, SecureDrop, encrypted email, or anonymous submission platforms are likely in *pre-disclosure* stages.

H2 — Employees experiencing retaliation after reporting misconduct are high-probability whistleblowers.
Patterns such as suspension, demotion, HR complaints, unexplained role changes, or legal retaliation strongly correlate with later public disclosures.

H3 — Anonymous posts describing internal wrongdoing often precede formal whistleblowing.
Users on Reddit, Tor forums, and industry-specific communities who describe fraud, safety violations, exploitation, or discrimination but avoid identifying themselves often match early signalling behaviour.

H4 — Public frustration toward an organisation indicates readiness for disclosure.
Individuals who repeatedly criticize an employer or institution online—especially through long-form posts, evidence-sharing, or appeals to journalists—may be transitioning from internal reporting to external whistleblowing.

2. Investigative Findings

2.1 Understanding the mindset of a whistleblower

Whistleblowing is rarely a spontaneous or reckless act. It is a deliberate moral decision, driven by individuals who find themselves at the crossroads between loyalty and justice. A whistleblower's mindset is deeply anchored in personal ethics, courage, and an internal sense of right and wrong that compels them to act, even when it means risking their reputation, career, or safety.

According to *The Whistleblower's Dilemma: The Fairness–Loyalty Tradeoff*, individuals who expose wrongdoing often experience a psychological conflict between fairness and loyalty. The decision to report unethical behavior is not motivated by disobedience or rebellion, but by a powerful sense of justice and the belief that integrity must take precedence over blind allegiance to authority. *article*

However, courage comes with consequences. Whistleblowers face elevated levels of depression, anxiety, and social isolation compared to the general population. The same study found that many whistleblowers experience retaliation, professional exclusion, and a loss of trust in social and professional relationships.

A recent 2024 study in *Sage Journals* revealed that whistleblowers often share a distinct set of personality traits, including high conscientiousness, openness to experience, and a low tolerance for unethical authority. These individuals demonstrate strong internal control, self-efficacy, and independence from group conformity, which enables them to challenge entrenched systems of power. *Sage-journals*

2.2 Environments that create whistleblowers

Whistleblowers often emerge from complex, high-stakes environments where power, secrecy, and ethical ambiguity coexist. Such settings foster conditions where wrongdoing is easily concealed, oversight is limited, and individuals with strong moral frameworks find themselves in ethical conflict with their surroundings.

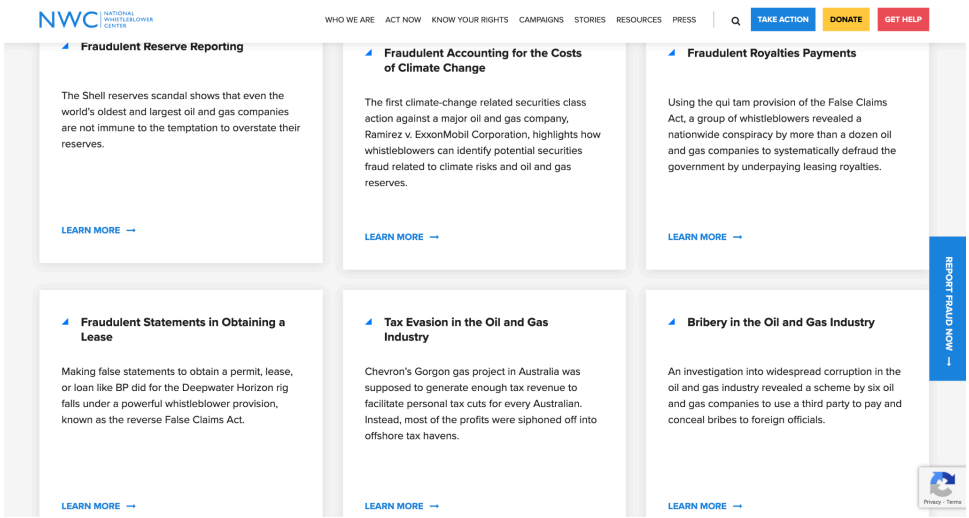
- The mining and resource extraction industries exemplify this tension. These sectors involve large-scale environmental and safety risks, political influence, and complex licensing systems. A report by Falcony highlights several cases where insiders disclosed corruption, falsified safety audits, and environmental cover-ups in major mining corporations. In these environments, transparency is often sacrificed in favor of profit and political convenience, creating moral pressure for insiders to act. *falcony article*
- A study on the Nigerian extractive industry further emphasizes that whistleblowing mechanisms are frequently underdeveloped, leaving employees exposed to retaliation and without institutional protection. *nigerian whistleblowing measures*

In Nigeria, there is no whistle-blowing law, thus individuals and civil society groups cannot provide confidential (environmental) information publicly (Ekhator 2013; Ekhator 2014). This is mainly due to the fear of retaliation and lack of protection for coming forward with legitimate disclosures about wrongdoing. For example, in 2013 a whistle-blower who exposed a series of (alleged) corrupt activities by the Minister of Aviation was threatened with prosecution because according to a senior government official, the whistle-blower's action was tantamount to a criminal offence (Sahara reporters 2013).

Furthermore, many of the laws regulating the extractive industry in Nigeria have little or no provisions for protecting whistle-blowers (Ekhator 2014). For example, section 1 of the Harmful Wastes (Special Criminal Provisions) Act (2004) prohibits the illegal dumping of hazardous wastes in Nigeria. Unfortunately, this law provides no protection for whistle-blowers who report incidence of hazardous dumping by companies in the extractive industry (Ekhator 2014). If an employee raises an alarm about hazardous dumping of waste, such an employee has no protection under the law in the Nigerian extractive industry and the 'employee can be dismissed and many of the existing laws provides no remedy for such an

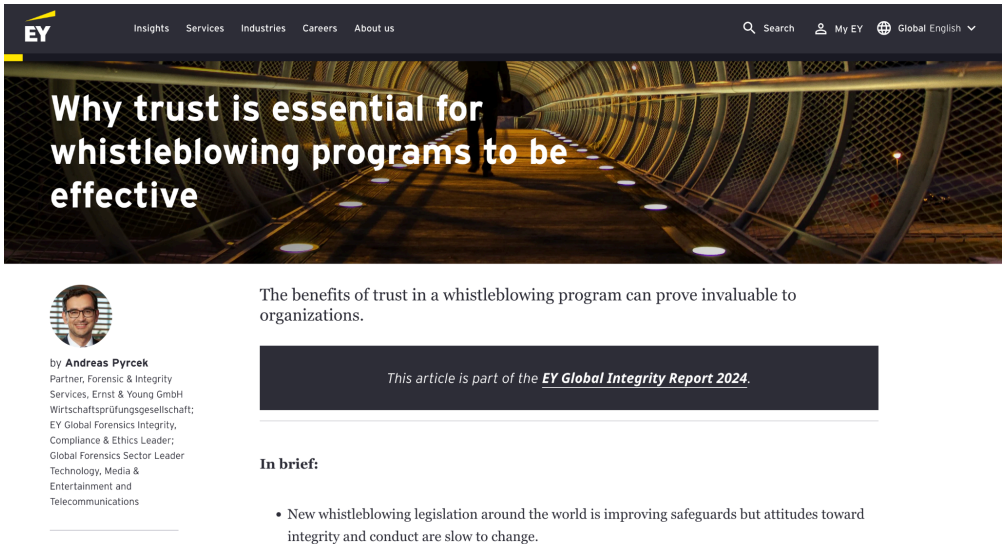
Nigeria's No whistle-blowing law article

- The oil and gas industry represents another high-risk environment where ethical challenges are systemic. The *National Whistleblower Center* reports numerous cases involving falsified emissions data, bribery of officials, and concealment of environmental hazards. Because these corporations often operate across multiple jurisdictions, accountability mechanisms are fragmented, allowing corruption and negligence to persist. In such contexts, morally driven employees become the last line of accountability, often exposing misconduct at great personal cost.

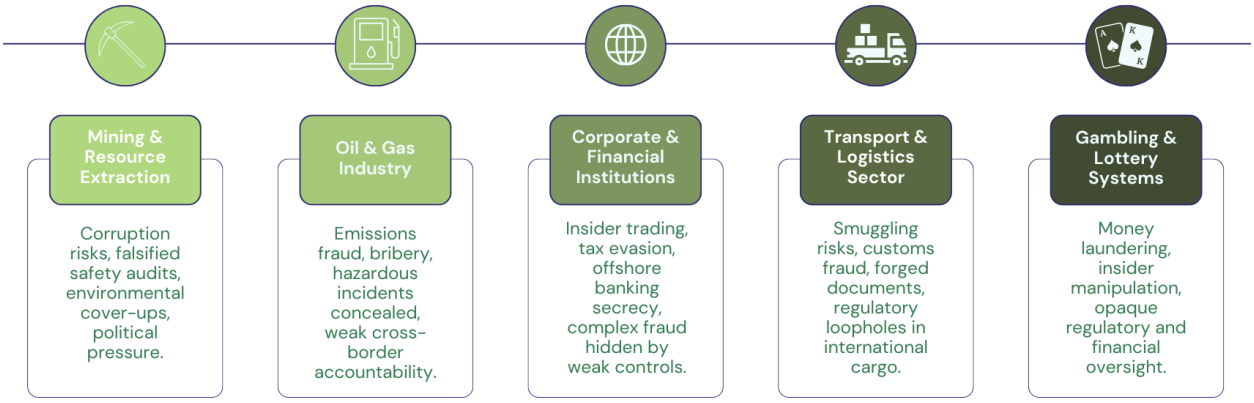


National Whistleblower Centre's Oil & Gas Case Studies

- Corporate and financial institutions, especially those dealing with offshore banking, also serve as breeding grounds for whistleblowers. These organizations handle vast sums of money, often through complex and opaque financial structures. Misconduct such as insider trading, tax evasion, and fraudulent reporting can remain undetected for years due to weak internal controls. The global reach of offshore financial centers makes regulatory enforcement inconsistent, forcing ethical employees to act as informal watchdogs. *ey report*



- Industries such as air and sea cargo transport, lotteries, and casinos may appear unrelated but share similar structural weaknesses. In transport, the potential for smuggling, customs fraud, and document falsification creates fertile ground for ethical breaches. Lotteries and casinos, governed by both public and private interests, are particularly vulnerable to money laundering, insider manipulation, and regulatory violations. Employees who witness these activities often find themselves in moral and legal conflict, especially when their institutions suppress or ignore complaints.



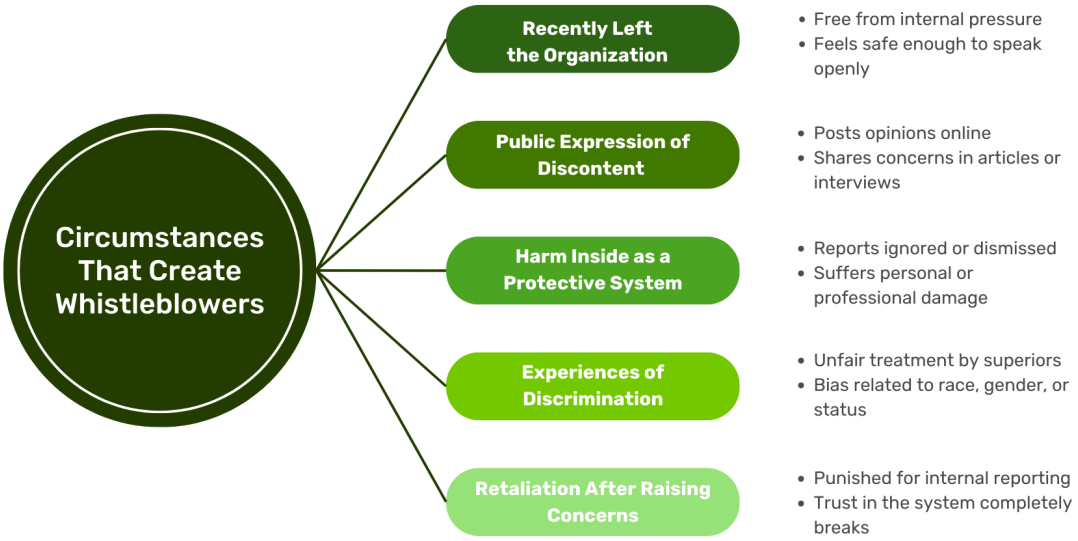
Across all these sectors, a pattern emerges. Whistleblowers are most likely to surface where there is operational opacity, high financial or environmental stakes, limited oversight, and internal cultures that discourage dissent. The greater the imbalance between public transparency and insider knowledge, the stronger the conditions that produce individuals willing to expose the truth.

2.3 Circumstances that Could Create Whistleblowers

Whistleblowers emerge from pressure, injustice, and lived experiences that steadily push them toward disclosure. Most people do not begin with the intention to expose wrongdoing. They reach that point only after the systems around them fail repeatedly. When someone's concerns are ignored, when accountability mechanisms collapse, or when harm continues unchecked, individuals slowly shift from silent observers to active truth tellers.

Often these are people who first tried to follow internal procedures. They reported issues to supervisors, filed complaints, or trusted formal channels to do what was right. When nothing changes, the emotional and ethical weight builds. Witnessing ongoing damage, discrimination, or corruption creates a sense of responsibility that becomes impossible to suppress.

What starts as frustration becomes a moral obligation. The person begins to understand that speaking up publicly may be the only way to stop the wrongdoing. These moments of personal crisis and ethical awakening form the circumstances that commonly lead someone toward whistleblowing.



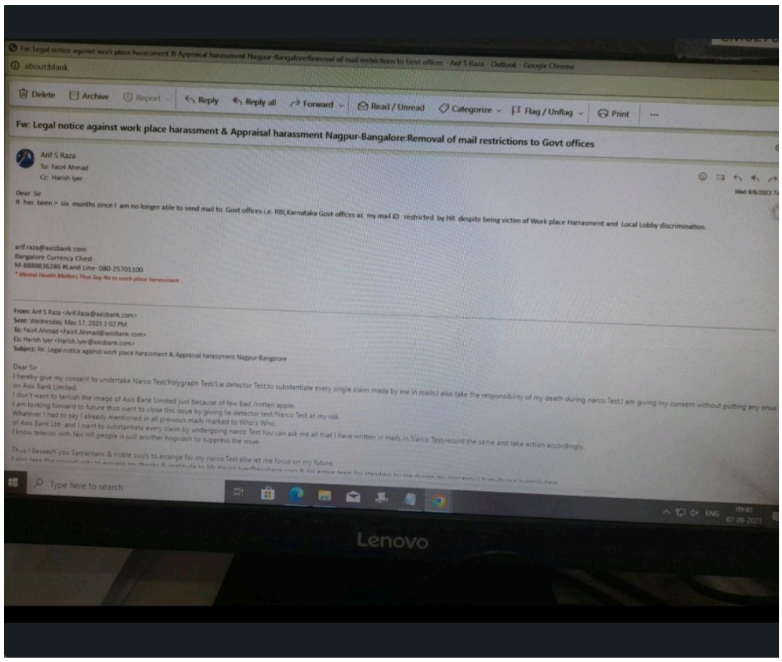
2.4 Identifying Potential Whistleblowers on Social Media

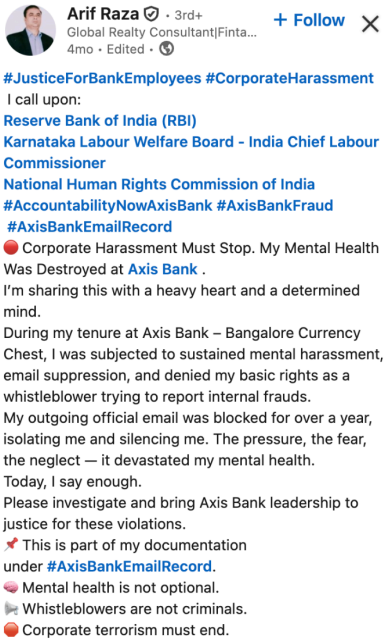
Social media platforms have become one of the most visible environments in which whistleblowing activity emerges. Unlike traditional reporting channels that are formal, confidential, and often bureaucratic, social media platforms allow individuals to speak in their own voices, in real time, and directly to the public. These platforms enable potential whistleblowers to express dissatisfaction, describe harms, and document retaliation long before formal investigations or media coverage take place. As a result, social media forms an early-signal environment where emerging ethical conflicts can be observed and analyzed through open-source intelligence techniques.

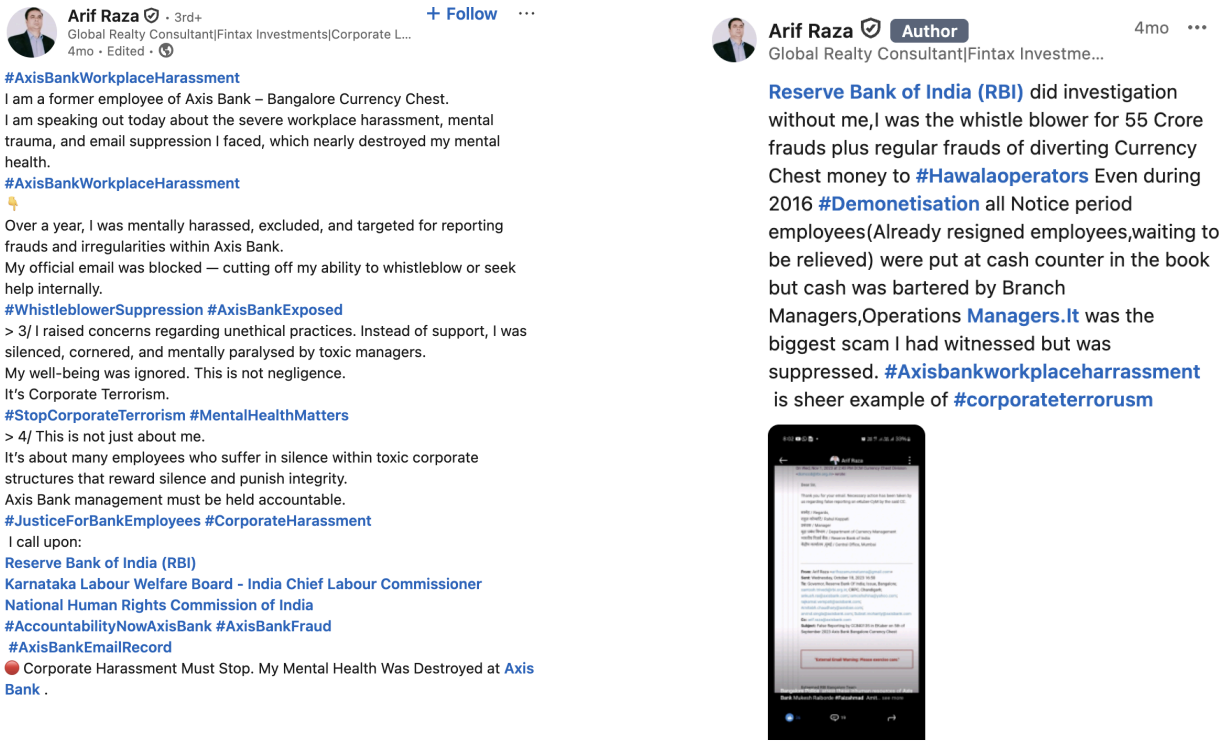
Individuals who disclose wrongdoing online often do so after internal reporting mechanisms have failed or been actively suppressed. The public post becomes a form of last-resort accountability, where the whistleblower seeks validation, support, or simply a record that their concerns were voiced.

Axis Bank Whistleblower – Arif Raza

A former employee of Axis Bank publicly disclosed detailed allegations of financial misconduct and systematic harassment within the organization through a series of LinkedIn posts. Raza reports that he attempted to raise internal alerts regarding fraud within the bank's currency chest division, including allegations of diverted funds and irregular handling of cash during the 2016 demonetization period. Rather than being protected or supported, he describes being subjected to email suppression, social isolation, mental harassment, and removal of workplace access, leaving him unable to communicate with oversight authorities.







Arif Raza exposing Axis Bank

His posts include images of official correspondence, which strengthens the credibility of his claims and demonstrates a willingness to place verifiable documentation in the public domain. Raza frames his experience not as an isolated employment grievance but as part of a broader cultural problem in which organizational loyalty is valued above ethical conduct, resulting in severe personal and psychological harm to individuals who attempt to act in the public interest.

Privacy Breach Whistleblowing in Canada – Aaruni Abhishek

Aaruni Abhishek reported identifying a significant privacy flaw within one of Canada's largest banks, TD Bank, that allegedly exposed sensitive customer information. He states that instead of receiving legal or institutional protection after raising the issue internally, he experienced professional retaliation, including pay disruption, loss of responsibilities, and eventual termination.

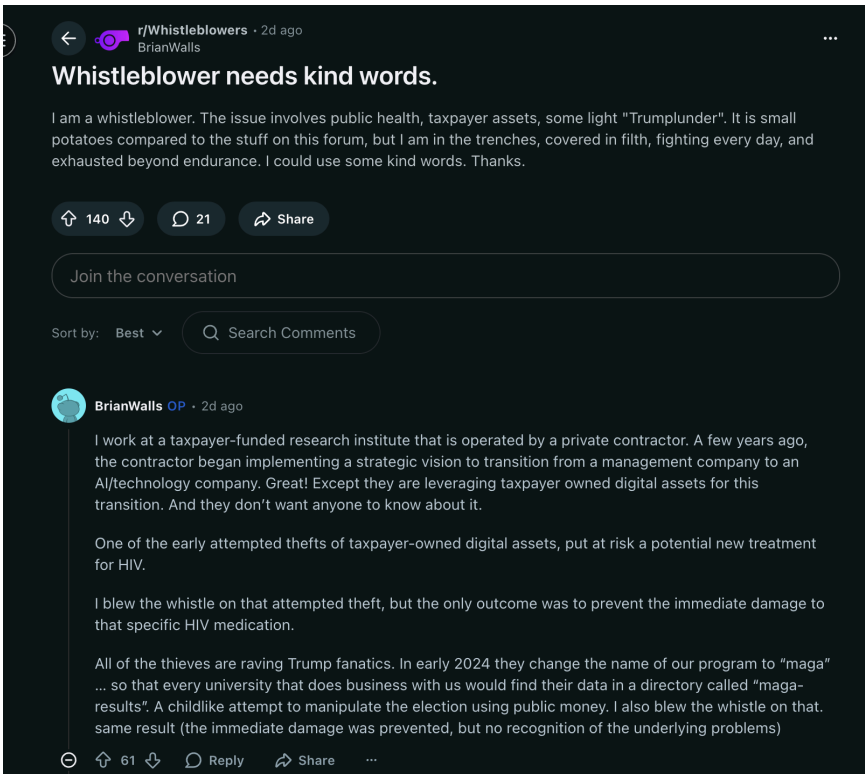
After escalation to the Office of the Privacy Commissioner, he reports that the case was dismissed due to a regulatory loophole that fails to act unless the whistleblower's own personal data is involved. His post underscores a systemic vulnerability in Canada's privacy enforcement structure, where organizational misconduct may go unaddressed despite posing risk to large numbers of customers. *Lin*

kedin

Anonymous Insider Disclosure – Reddit r/Whistleblowers

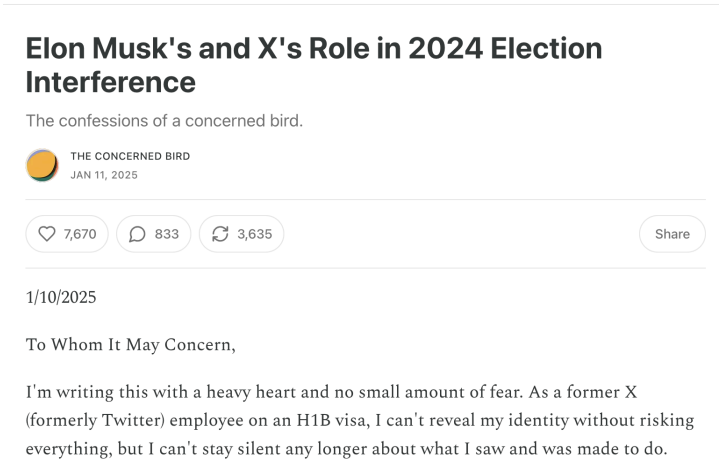
In a Reddit post under r/Whistleblowers, an individual describes being employed at a taxpayer-funded research institute operated by a private contractor. The whistleblower reports that digital assets related to public health research were being repurposed for private technological and political objectives without public knowledge. The post further describes failed internal whistleblowing attempts, emotional exhaustion, and the absence of institutional accountability mechanisms. The anonymity of Reddit allows disclosures at an

earlier emotional stage, where the whistleblower seeks psychological support and peer validation rather than formal legal remedy.



r/Whistleblowers

Former X (Twitter) Employee Alleging Political Manipulation

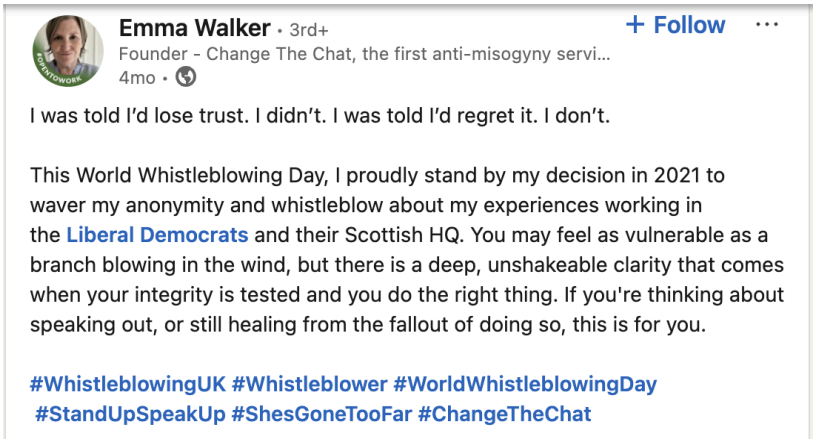


A pseudonymous Substack article written by a former X (Twitter) employee alleges deliberate algorithmic manipulation to influence the 2024 U.S. presidential election. The writer claims that platform-level decisions were made to artificially amplify political messaging in favor of specific candidates. The author identifies themselves as working under an H1B visa, which creates heightened vulnerability and explains their use of anonymity.

Substack, by design, provides long-form narrative space that allows whistleblowers to construct timelines, justify context, and articulate harm in ways that shorter platforms do not afford. This case represents the genre of whistleblowing where **policy influence intersects with technological power**, which is increasingly significant in the modern information ecosystem. *substack*

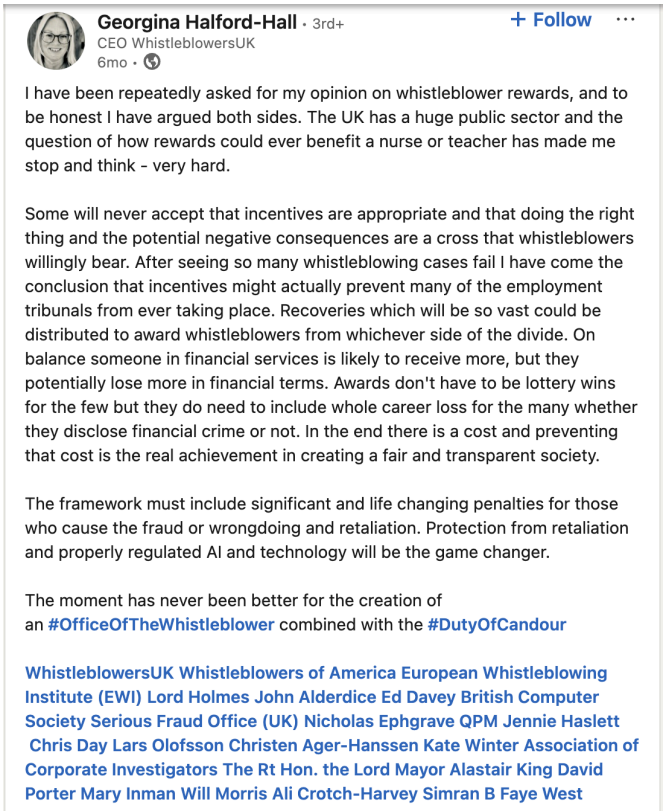
Workplace Harassment and Political Whistleblowing in a UK Political Party – Emma Walker

Emma Walker describes whistleblowing about misogynistic workplace abuse within the Scottish Liberal Democrats' organizational environment. Her post reflects the *aftermath stage* of whistleblowing, where the primary disclosure has already occurred, and the speaker is now publicly reclaiming narrative agency and personal identity. Her tone emphasizes resilience, moral clarity, and emotional recovery. *linkedin*



Policy Advocacy and Whistleblowing Reform – Georgina Halford-Hall

Georgina Halford-Hall, CEO of WhistleblowersUK, uses LinkedIn to argue the case for structured whistleblowing rewards and legal reform. Her post underscores the structural and cultural barriers that discourage whistleblowing, noting that even when disclosures are validated, whistleblowers often experience career destruction, financial loss, and identity disruption. *linkedin*



Georgina Halford-Hall · 3rd+ + Follow ···
CEO WhistleblowersUK
6mo ·

I have been repeatedly asked for my opinion on whistleblower rewards, and to be honest I have argued both sides. The UK has a huge public sector and the question of how rewards could ever benefit a nurse or teacher has made me stop and think - very hard.

Some will never accept that incentives are appropriate and that doing the right thing and the potential negative consequences are a cross that whistleblowers willingly bear. After seeing so many whistleblowing cases fail I have come the conclusion that incentives might actually prevent many of the employment tribunals from ever taking place. Recoveries which will be so vast could be distributed to award whistleblowers from whichever side of the divide. On balance someone in financial services is likely to receive more, but they potentially lose more in financial terms. Awards don't have to be lottery wins for the few but they do need to include whole career loss for the many whether they disclose financial crime or not. In the end there is a cost and preventing that cost is the real achievement in creating a fair and transparent society.

The framework must include significant and life changing penalties for those who cause the fraud or wrongdoing and retaliation. Protection from retaliation and properly regulated AI and technology will be the game changer.

The moment has never been better for the creation of an #OfficeOfTheWhistleblower combined with the #DutyOfCandour

WhistleblowersUK Whistleblowers of America European Whistleblowing Institute (EWI) Lord Holmes John Alderdice Ed Davey British Computer Society Serious Fraud Office (UK) Nicholas Ephgrave QPM Jennie Haslett Chris Day Lars Olofsson Christen Ager-Hanssen Kate Winter Association of Corporate Investigators The Rt Hon. the Lord Mayor Alastair King David Porter Mary Inman Will Morris Ali Crotch-Harvey Simran B Faye West

---

Collective Whistleblowing – FEMA Employees Open Letter

The FEMA employees' collective letter demonstrates how whistleblowing can be distributed rather than individual, especially in governmental contexts. Collective whistleblowing reduces personal risk but indicates severe structural risk when large numbers of internal staff report the same issue simultaneously. This case strengthens your argument that whistleblowing scales with systemic failure. *whistleblowers blog*

On October 14th, the Committee on Transportation & Infrastructure and the Subcommittee on Public Buildings, Economic Development, and Emergency Management sent a letter to Inspector General Joseph Cuffari and Senior Official of the Federal Emergency Management Agency (FEMA) David Richardson, addressing their “continued alarm” regarding the termination of whistleblowers at FEMA.

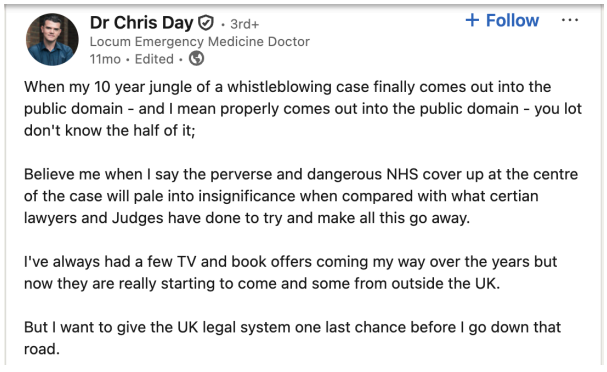
The letter was in reference to an open letter signed by 192 FEMA employees on August 25th, warning Congress of the Trump Administration’s overreaching imposition. The letter, entitled the Katrina Declaration, delineated the six primary ways in which the Trump Administration is “putting lives at risk by undermining FEMA’s ability to perform disaster response and recovery.”

In the Katrina Declaration, FEMA employees expressed unease over the current leadership’s lack of qualifications, the reduction in funding, and the censorship of climate research, to name a few. As CNN highlighted, the current Senior Official at FEMA, David Richardson, is “a former Marine combat veteran with no prior experience managing natural disasters.” By his side are equally “inexperienced aides,” CNN claims. Moreover, the Katrina Declaration underscores that incentives for employees to leave the service are so grave that “one-third of FEMA’s full-time staff” have thus far departed. Additionally, FEMA employees have been explicitly told to remove any information about climate change from both public-facing and internal documents, an instruction the employees claim violates *The Community Disaster Resilience Zones Act of 2022*.

An excerpt from blog

Long-Term Whistleblower Legal Struggle – Dr. Chris Day

Dr. Chris Day describes a prolonged legal struggle after exposing patient safety concerns in the UK’s National Health Service. His post indicates that whistleblowing frequently involves extended litigation, reputational hardship, and systemic resistance rather than immediate acknowledgment or reform. His narrative adds longitudinal evidence of whistleblower retaliation and survival. *linkedin*



Dr Chris Day · 3rd+ + Follow ···
Locum Emergency Medicine Doctor
11mo • Edited •

When my 10 year jungle of a whistleblowing case finally comes out into the public domain - and I mean properly comes out into the public domain - you lot don't know the half of it;

Believe me when I say the perverse and dangerous NHS cover up at the centre of the case will pale into insignificance when compared with what certian lawyers and Judges have done to try and make all this go away.

I've always had a few TV and book offers coming my way over the years but now they are really starting to come and some from outside the UK.

But I want to give the UK legal system one last chance before I go down that road.

2.5 Identifying Potential Whistleblowers on Online Communities

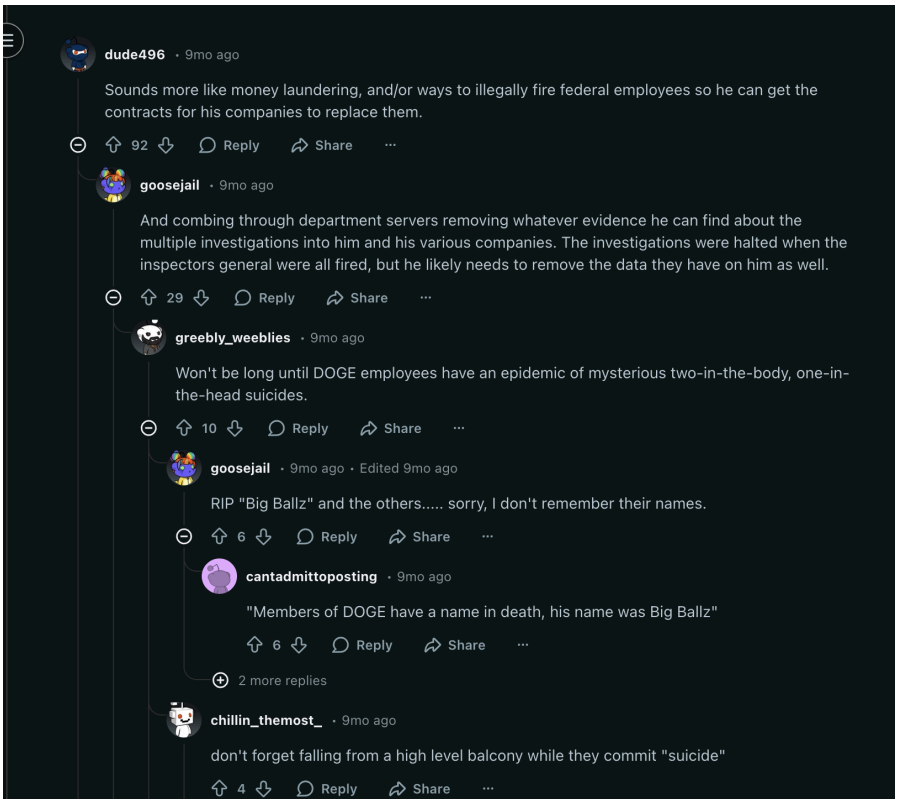
Online communities such as Reddit and anonymous forums often act as early staging grounds for whistleblowing. Because users can speak without revealing their identities, these spaces frequently contain the first signs of ethical conflict, frustration, or intent to report wrongdoing. Individuals use these platforms to describe internal issues, seek legal or technical advice, and ask how to contact journalists or use secure communication tools.

These discussions are valuable because they reveal emerging whistleblower behaviour before it becomes public or formal. Patterns of repeated complaints, mentions of retaliation, or requests for safe reporting methods can indicate individuals preparing to disclose misconduct. The following cases show how online communities allow whistleblowers to express concerns, gather support, and navigate the early steps of exposing wrongdoing.

Anonymous Allegations About DOGE Manipulation

An *anonymous post* on r/Whistleblowers claims that Elon Musk is manipulating DOGE-related performance results to hide internal failures. Although the post provides no evidence, the discussion quickly turns into a thread where multiple users describe patterns of misconduct, including accusations of money laundering, illegal terminations, evidence removal from federal department servers, and halted investigations.

The comment chain reflects a community openly discussing serious wrongdoing and retaliation fears, with users referencing sudden staff dismissals, suppressed oversight, and risks faced by employees involved in the DOGE program.

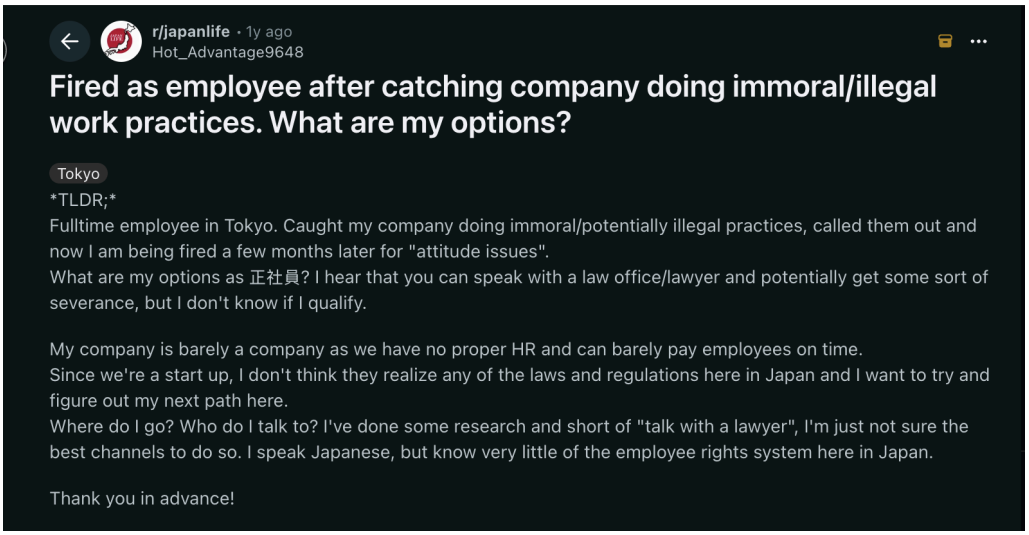


Thread on r/Whistleblowers

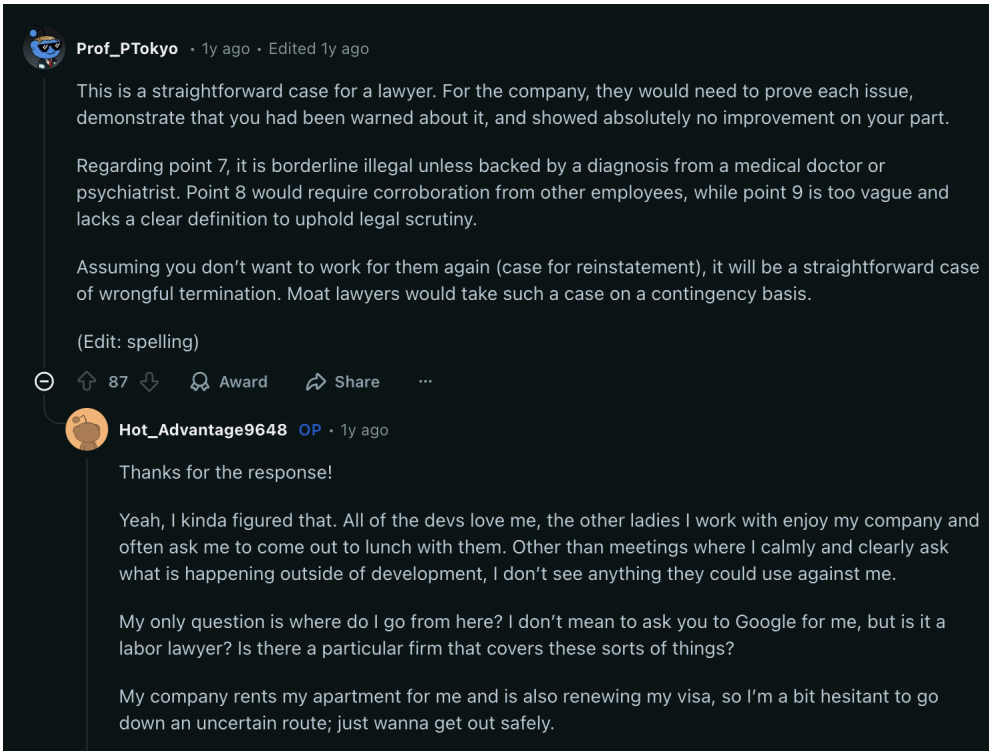
Employee Fired After Reporting Illegal Practices in a Tokyo Start-up

A user in r/japanlife *reported being dismissed* shortly after confronting their start-up employer about immoral and potentially illegal business practices. According to the post, the company had been using fake listings to inflate its market image, and when the employee raised concerns, they were later fired for vague “attitude issues.” The user explains that the company has no proper HR structure, struggles to pay staff on time, and appears unaware of Japanese labour regulations, leaving the employee uncertain about their rights and next steps.

In the discussion thread, commenters identify the situation as a likely wrongful termination case and advise the poster to consult a labour lawyer.



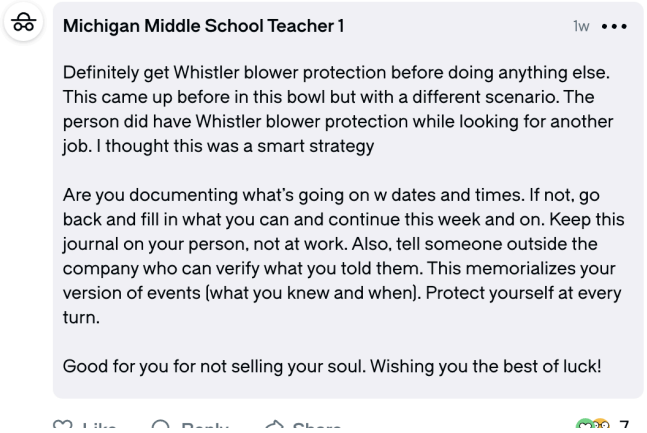
正社員 - *full time employee*



An Anonymous Director Seeking Whistleblower Advice on Glassdoor's The Worklife Bowl Community

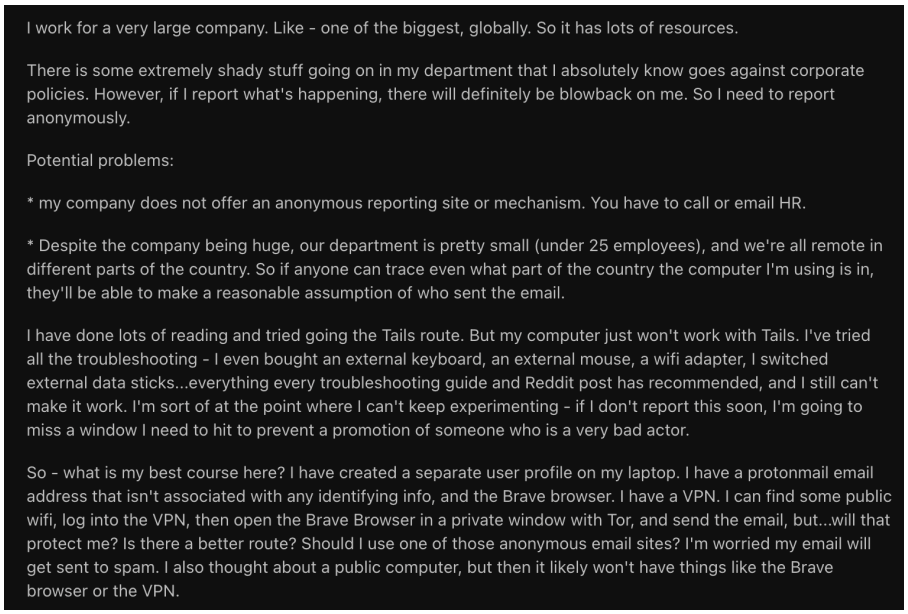
A user posted anonymously about discovering *serious data misuse* within their company. According to the post, the organisation was repurposing licensed data for other clients, including competitors, secretly recording customers on-site, and fabricating data for sale. The user expressed concern that raising these issues would likely lead to termination and asked whether they should act pre-emptively and whistleblow.

The comment section reflects a strong consensus that the situation involves significant legal and ethical violations. Other users advised the poster to document everything, avoid discussing the matter internally, consult a lawyer, and secure whistleblower protection before taking action.



Anonymous User Seeking Safe Whistleblowing Methods on r/TOR

A user on r/TOR described witnessing serious *misconduct in a large global company* and expressed fear of retaliation if they reported it internally. The company offered no anonymous reporting mechanism, and because the department was small, the poster believed any report could be traced back to them. The individual attempted to use Tails OS to submit an anonymous complaint but struggled with technical issues, prompting them to ask the community for advice on secure alternatives.



I work for a very large company. Like - one of the biggest, globally. So it has lots of resources.

There is some extremely shady stuff going on in my department that I absolutely know goes against corporate policies. However, if I report what's happening, there will definitely be blowback on me. So I need to report anonymously.

Potential problems:

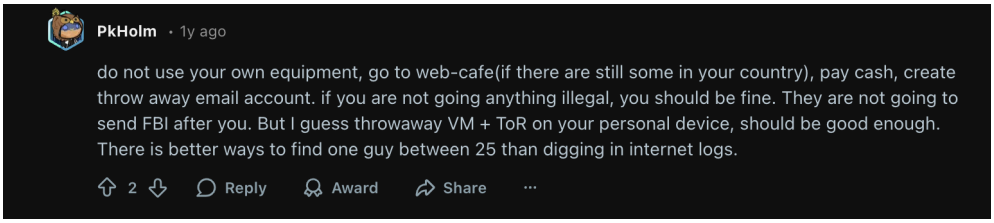
* my company does not offer an anonymous reporting site or mechanism. You have to call or email HR.

* Despite the company being huge, our department is pretty small (under 25 employees), and we're all remote in different parts of the country. So if anyone can trace even what part of the country the computer I'm using is in, they'll be able to make a reasonable assumption of who sent the email.

I have done lots of reading and tried going the Tails route. But my computer just won't work with Tails. I've tried all the troubleshooting - I even bought an external keyboard, an external mouse, a wifi adapter, I switched external data sticks...everything every troubleshooting guide and Reddit post has recommended, and I still can't make it work. I'm sort of at the point where I can't keep experimenting - if I don't report this soon, I'm going to miss a window I need to hit to prevent a promotion of someone who is a very bad actor.

So - what is my best course here? I have created a separate user profile on my laptop. I have a protonmail email address that isn't associated with any identifying info, and the Brave browser. I have a VPN. I can find some public wifi, log into the VPN, then open the Brave Browser in a private window with Tor, and send the email, but...will that protect me? Is there a better route? Should I use one of those anonymous email sites? I'm worried my email will get sent to spam. I also thought about a public computer, but then it likely won't have things like the Brave browser or the VPN.

In the replies, users warned against using work devices, advised reporting only from neutral locations, and suggested disposable accounts, VPNs, and non-company hardware. Others shared experiences where corporate “anonymous” hotlines exposed complainants, reinforcing the user’s concern. This thread clearly reflects a potential whistleblower actively searching for safe communication channels and troubleshooting anonymity tools before disclosure.



PkHolm · 1y ago

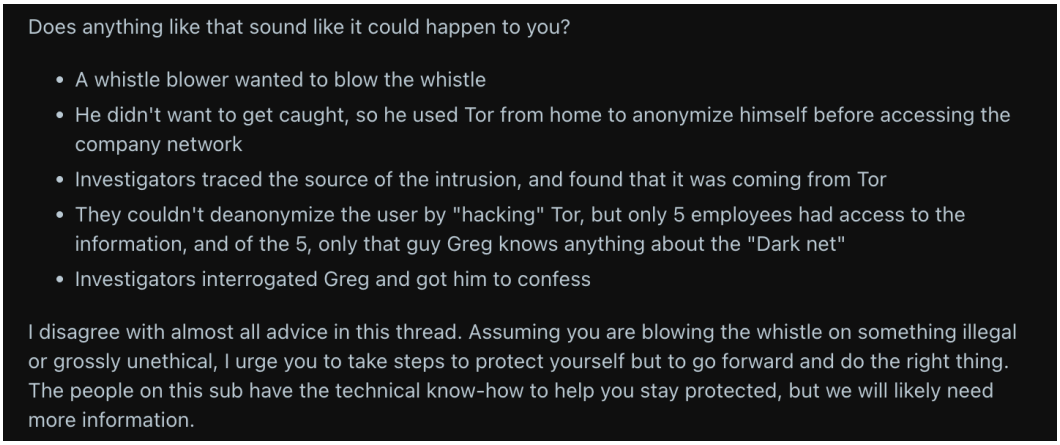
do not use your own equipment, go to web-cafe(if there are still some in your country), pay cash, create throw away email account. if you are not going anything illegal, you should be fine. They are not going to send FBI after you. But I guess throwaway VM + ToR on your personal device, should be good enough. There is better ways to find one guy between 25 than digging in internet logs.

2 Reply Award Share ...

User Considering Data Leak via Tor as a Whistleblowing Method

An older post in r/TOR shows a user *planning to leak* internal company data using Tor and a throwaway email address. The individual asks whether Tor alone is enough to stay anonymous throughout the whistleblowing process. This represents a direct attempt to find secure communication channels while preparing to expose corporate wrongdoing.

The replies caution the user that Tor by itself does not guarantee anonymity if the whistleblower accesses data from identifiable devices or company networks. Commenters reference real incidents where individuals were traced not through Tor, but through contextual clues such as unique access patterns. The thread also highlights safer alternatives like using Tails OS and SecureDrop to protect identity.



Does anything like that sound like it could happen to you?

- A whistle blower wanted to blow the whistle
- He didn't want to get caught, so he used Tor from home to anonymize himself before accessing the company network
- Investigators traced the source of the intrusion, and found that it was coming from Tor
- They couldn't deanonymize the user by "hacking" Tor, but only 5 employees had access to the information, and of the 5, only that guy Greg knows anything about the "Dark net"
- Investigators interrogated Greg and got him to confess

I disagree with almost all advice in this thread. Assuming you are blowing the whistle on something illegal or grossly unethical, I urge you to take steps to protect yourself but to go forward and do the right thing. The people on this sub have the technical know-how to help you stay protected, but we will likely need more information.

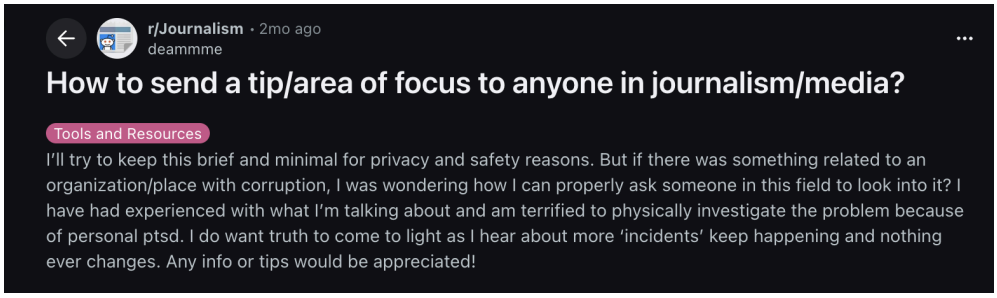
2.6 Identifying Potential Whistleblowers on Dark Web

The dark web can be a space where individuals anonymously seek help, guidance, or secure channels to expose wrongdoing. While usernames and identities are hidden, the content of their posts, the nature of their concerns, and the platforms they engage with can reveal patterns similar to those found on the surface web. By comparing the themes, terminology, and context of these discussions, it becomes possible to identify individuals who may be preparing to whistleblow.

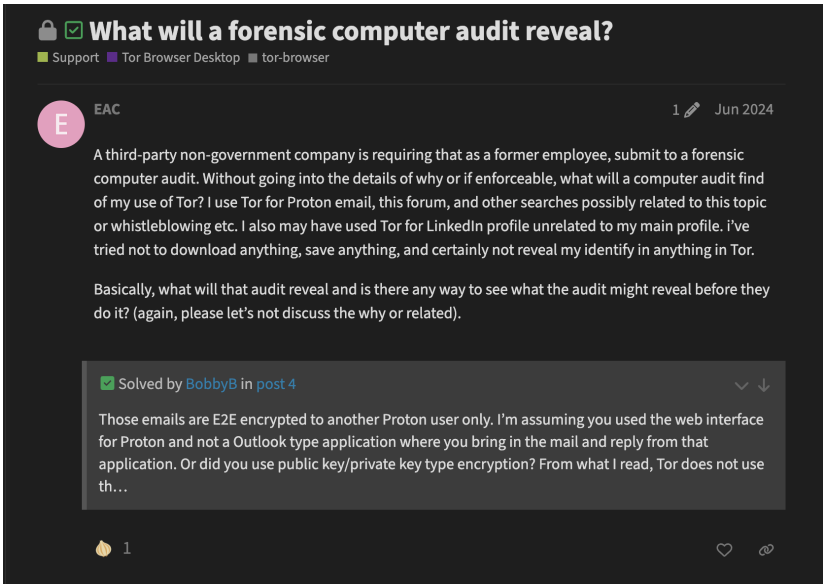
A post from **r/employmenttribunal** shows a user publicly identifying themselves as a *whistleblower* and describing the aftermath of multiple tribunal cases and a criminal proceeding. They explain that the lack of consistent support frameworks led them to create a dedicated community for whistleblowers, titled ***r/WhistleblowerCompass***, aimed at offering structured guidance for individuals navigating similar situations.

The user introduces themselves as a Regulated Risk and Compliance Officer and highlights themes such as confidentiality, ethics, and fair justice as core principles of their advocacy.

A user on **r/Journalism** asks how to safely provide *information to reporters* about corruption within an organization. The post shows clear hesitation due to privacy concerns and past traumatic experiences. The individual stresses wanting "truth to come to light" but fears directly investigating the issue themselves. This type of inquiry reflects early-stage whistleblower behavior, where someone is exploring safe channels to disclose sensitive information to the media without exposing their identity.

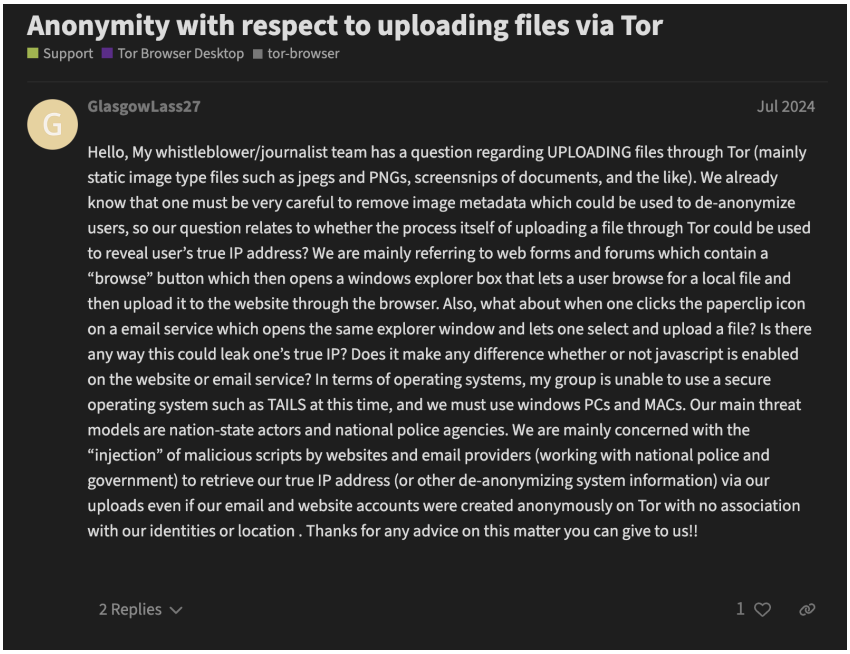


A user on a **Tor support forum** asks what a forensic computer audit might reveal about their past use of Tor. They mention using Tor for ProtonMail, forums, and searches related to whistleblowing, and express clear fear about their identity being exposed during the audit. This indicates an individual actively trying to protect themselves after raising or planning to raise concerns about misconduct. *tor forum*



A user on **r/onions** expresses fear about using Tor for the first time specifically to ***search for whistleblower content***. They are worried about accidentally accessing illegal sites and ask how to protect their identity while researching whistleblowing information. The user's caution, anonymity concerns, and intent to browse whistleblower-related material suggest they may be exploring ways to report or expose wrongdoing while remaining untraceable.

A user on a Tor forum describes working with a **whistleblower/journalist team** and asks whether *uploading files through Tor* could expose their real IP address. They express concern about metadata, browser behavior, JavaScript, and potential deanonymization by state-level actors. The detailed focus on secure file submission indicates active attempts to safely transfer whistleblower materials while avoiding identification.



2.7 Discovering Support Information that Promotes Whistleblowing

Note on Source Variability Within Whistleblower Discussions

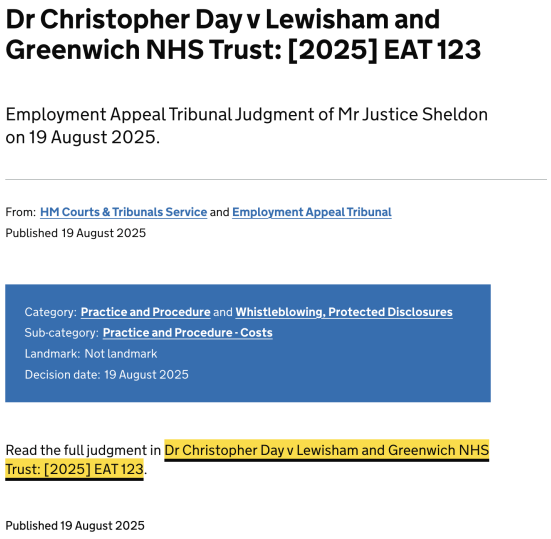
Across the communities analysed, many individuals discussing whistleblowing deliberately maintain a high level of anonymity. These users typically ask general questions about reporting mechanisms, legal protections, or technical methods to remain anonymous (e.g., Tor, VPN use, secure file uploads). Because they avoid revealing details about their employer, industry, region, or the nature of the misconduct, their posts cannot be linked to external evidence or verified through additional OSINT sources.

However, a smaller set of users provide enough organisational context to allow cross-checking against independent information. For these cases, it is possible to identify supporting evidence from news reports, regulatory actions, legal documents, and prior public allegations involving the organisation or sector.

Dr Christopher Day – NHS Whistleblowing Dispute

Multiple authoritative sources back the long-running whistleblowing case involving Dr Christopher Day, providing a well-documented example of how protected disclosures can evolve into major employment disputes. The available documents show that Dr Day raised patient-safety concerns during his employment with Lewisham and Greenwich NHS Trust, which led to an earlier tribunal in 2014.

The evidence from the *Employment Tribunal* summary notes that Dr Day later alleged detriment due to the Trust's actions and statements surrounding his protected disclosures. The Tribunal acknowledged that one of the statements made by the NHS Trust *did* amount to a detriment, but it concluded the detriment was not caused by his whistleblowing activity. It also ruled that certain alleged detriments fell outside the scope of whistleblowing protection because they occurred after his employment ended.



Dr Christopher Day v Lewisham and Greenwich NHS Trust: [2025] EAT 123

Employment Appeal Tribunal Judgment of Mr Justice Sheldon on 19 August 2025.

From: HM Courts & Tribunals Service and Employment Appeal Tribunal
Published 19 August 2025

Category: Practice and Procedure and Whistleblowing, Protected Disclosures
Sub-category: Practice and Procedure - Costs
Landmark: Not landmark
Decision date: 19 August 2025

Read the full judgment in Dr Christopher Day v Lewisham and Greenwich NHS Trust: [2025] EAT 123.

Published 19 August 2025

Further supporting information is available through the published Employment Appeal Tribunal judgment from August 2025. The judgment confirms that Dr Day appealed the tribunal's findings, and it provides an accessible, official record of the case.

As his tribunal case is finally heard, Chris Day discusses winning protection for other junior doctors – and why he feels betrayed

'It was incredible that so much effort was going into discrediting me and my safety concerns.' Chris Day in Woolwich, south east London. Photograph: Sarah Lee/The Guardian

Blowing the whistle in the NHS is meant to be easy. Medical bodies such as the Department of Health and Social Care, the General Medical Council (GMC) and individual hospital trusts all encourage the practice – on paper. But when Chris Day, a junior intensive care doctor, raised numerous concerns about understaffing and safety at the intensive care unit of Queen Elizabeth hospital in Woolwich, he found out all too quickly the toll it would take on his career.

Additional reporting from ***The Guardian*** reinforces the scale and seriousness of Dr Day's whistleblowing claims. The article highlights how, as a junior intensive care doctor at **Queen Elizabeth Hospital in Woolwich**, he raised repeated concerns about **dangerous understaffing and patient safety risks.**

Aaruni Abhishek vs TD Bank – Supporting Evidence & Corroboration

Aaruni Abhishek's whistleblowing claims revolve around internal privacy and security breaches at TD Bank, followed by alleged retaliation after he reported the issue through official channels. While the case is not as heavily covered in mainstream media as larger whistleblowing scandals, there *are* verifiable surface-web sources that confirm the existence of a legal dispute connected to his claims. *aaruni's blog*

aaruniabhishek · Aug 18 · 4 min read

Canada's Whistleblowing Dilemma: An Editorial on the Implications of the AARUNI Abhishek vs TD Case

In recent years, the issue of whistleblowing in Canada has come under intense scrutiny. The AARUNI Abhishek vs TD case , , has raised pivotal questions about the protections available to whistleblowers. As of 2025, the office of the privacy commissioner of canada has made it clear that it will not investigate complaints unless they directly affect the whistleblower. This decision has troubling implications, indicating that people in regulated sectors may think twice before reporting unethical or illegal actions, fearing they will not be shielded from backlash.

The repercussions of this ruling are immense, especially for employees in industries where ethical behavior is crucial. Whistleblowers serve as vital instruments for exposing wrongdoings like privacy breaches, financial fraud, and other unethical behavior. However, current policies in Canada raise significant doubts about the safety and security for those who decide to speak up.

One of the strongest pieces of supporting evidence comes from a ***2024 Ontario court decision***, reported by HR Law Canada, in which a judge ordered TD Bank to **produce unredacted internal complaint-investigation documents** in a wrongful dismissal case.
This directly aligns with Aaruni's public allegations that he filed complaints, raised concerns internally, and later faced retaliation and termination.

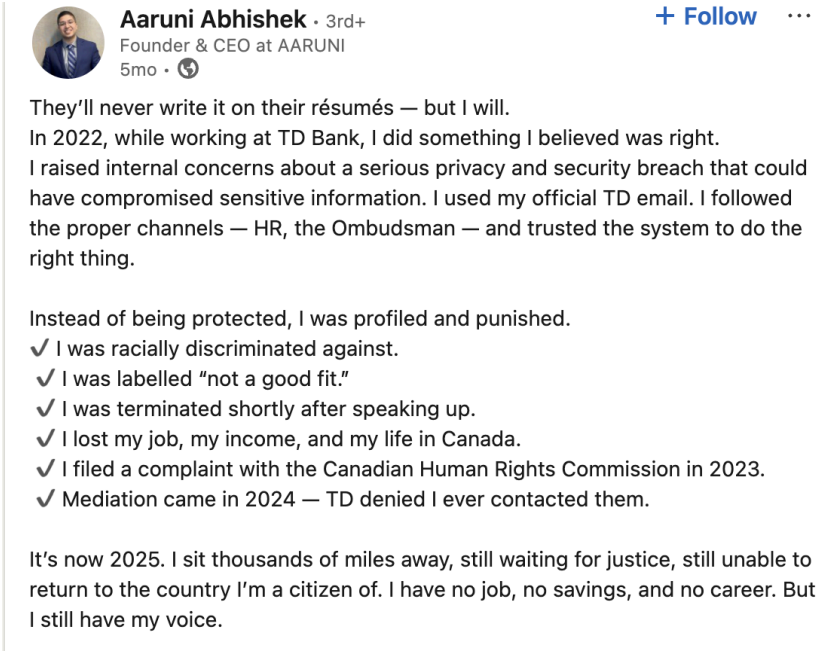
Ontario court orders TD Bank to produce unredacted complaints, workplace investigation documents

written by HR Law Canada | 9 July 2024 | A+A-

The Ontario Superior Court of Justice has ordered the Toronto-Dominion Bank (TD) to produce unredacted versions of employee complaints, a whistleblower complaint, and an investigation report in a wron…

Additionally, Aaruni's own public statements, through his *LinkedIn post* and long-form editorial provide detailed accounts of the events, the privacy breach he attempted to report,

the timeline of his termination, and his ongoing legal efforts through the **Canadian Human Rights Commission.**



Aaruni Abhishek · 3rd+
Founder & CEO at AARUNI
5mo ·

+ Follow ···

They'll never write it on their résumés — but I will.
In 2022, while working at TD Bank, I did something I believed was right.
I raised internal concerns about a serious privacy and security breach that could have compromised sensitive information. I used my official TD email. I followed the proper channels — HR, the Ombudsman — and trusted the system to do the right thing.

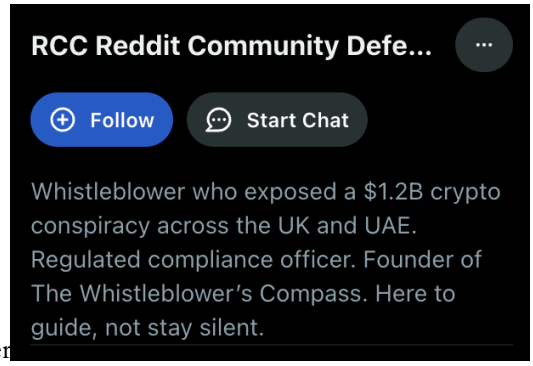
Instead of being protected, I was profiled and punished.
✓ I was racially discriminated against.
✓ I was labelled "not a good fit."
✓ I was terminated shortly after speaking up.
✓ I lost my job, my income, and my life in Canada.
✓ I filed a complaint with the Canadian Human Rights Commission in 2023.
✓ Mediation came in 2024 — TD denied I ever contacted them.

It's now 2025. I sit thousands of miles away, still waiting for justice, still unable to return to the country I'm a citizen of. I have no job, no savings, and no career. But I still have my voice.

Even though the story has not attracted widespread national coverage, **the combination of court filings, his public testimony, and legal reporting is substantial enough to validate the case** and support its inclusion within this investigation.

Anonymous Whistleblower Exposing a Large-Scale Fraud Scheme

This case involves a whistleblower who has chosen to remain anonymous. Although the individual has not disclosed their identity, the information they shared aligns closely with several authoritative public sources, which allows the claims to be verified without revealing who the whistleblower is. *Reddit Profile*



RCC Reddit Community Defe... ···

Follow Start Chat

Whistleblower who exposed a $1.2B crypto conspiracy across the UK and UAE. Regulated compliance officer. Founder of The Whistleblower's Compass. Here to guide, not stay silent.

darivxe - discover whistleblower

The anonymous informant described a major crypto related fraud operation affecting individuals across multiple countries. These allegations are strongly supported by official findings from the United States Attorney's Office for the Southern District of New York, which publicly confirmed the *arrest of Ho Wan Kwok*, also known as Miles Guo, for orchestrating a scheme valued at over one billion dollars. The official press release outlines extensive evidence of wire fraud, securities fraud and money laundering that matches the scale and behaviour described by the anonymous source. The information is available through the U S Department of Justice.

PRESS RELEASE

Ho Wan Kwok, A/K/A "Miles Guo," Arrested For Orchestrating Over $1 Billion Dollar Fraud Conspiracy

Wednesday, March 15, 2023

Share

For Immediate Release

U.S. Attorney's Office, Southern District of New York

Over $630 Million of Alleged Fraud Proceeds Seized by U.S. Government

Further independent journalistic investigations strengthen the credibility of this case. The Guardian reported on *Kwok's criminal trial* and detailed how he defrauded followers using a complex financial network.

Chinese business tycoon convicted of defrauding followers in $1bn scheme

Guo Wengui, who gained fans for criticizing Communist party in China, found guilty in US of nine criminal counts

The New York Times Magazine provided an in depth profile exploring his history, his influence and the web of allegations attached to his activities. Together, these reports substantiate the whistleblower's statements and demonstrate that the claims they shared reflect verified misconduct.


FEATURE

The Mystery of the Exiled Billionaire Whistle-Blower

From a penthouse on Central Park, Guo Wengui has exposed a phenomenal web of corruption in China's ruling elite — if, that is, he's telling the truth.

Although the whistleblower remains unidentified, the combination of legal documentation, investigative reporting and public testimony creates a clear and reliable picture of the underlying fraud. This makes the case an example of how anonymous disclosures can still be effectively validated through open source intelligence.

2.8 Reasoning for Classifying an Individual as a Potential Whistleblower

---

Dr. Chris Day (NHS)

Findings related to the organisation

The *Computer Weekly* investigation reports that Lewisham and Greenwich NHS Trust deleted thousands of emails connected to a major safety dispute. This behaviour suggests poor transparency during internal investigations, reinforcing Chris Day's earlier allegations of systemic mishandling of safety concerns.

How he was affected and motivated

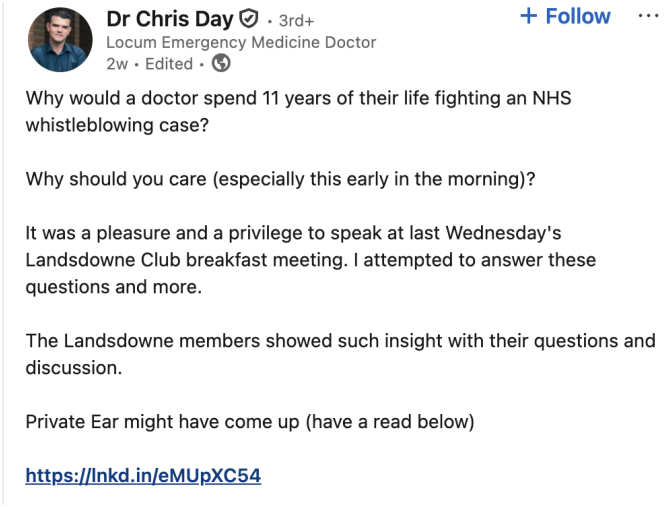
Chris Day raised concerns about unsafe staffing at Queen Elizabeth Hospital. Tribunal and media reports show that he faced attempts to discredit him and experienced significant career impact. These consequences strengthened his motivation to continue whistleblowing, seeking accountability for both patient safety issues and retaliation.

Indicators of intention

His pursuit of multiple tribunal hearings, appeals, and interviews demonstrates a deliberate commitment to exposing organisational failures. His continued legal escalation shows active involvement in whistleblowing processes.

Potential next steps

He may continue appealing tribunal outcomes, provide further evidence to oversight bodies, and collaborate with journalists covering NHS accountability issues.



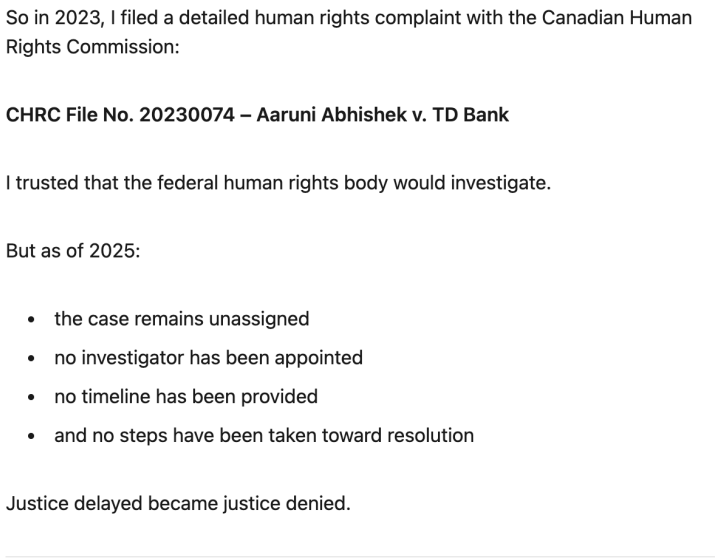
Aaruni Abhishek (TD Bank)

Findings related to the organisation

External reporting confirms that TD Bank has been under scrutiny for data security issues. Fox40's report on the *Levi and Korsinsky LLP* investigation shows that TD Bank suffered a data breach significant enough for potential class-action involvement. This supports the core claim in Aaruni's LinkedIn article, where he describes raising concerns about a serious privacy and security lapse inside the bank. The existence of an independent investigation strengthens the credibility of his initial warning.

How he was affected and motivated

Aaruni's own *published account* shows immediate and severe consequences after he reported the issue internally. He describes being racially profiled, labelled "not a good fit," and terminated shortly after raising his concerns. He lost his income, stability, and ultimately his legal ability to remain in Canada. His writing also states that his savings were drained while fighting the issue and that he was eventually forced to leave the country.



So in 2023, I filed a detailed human rights complaint with the Canadian Human Rights Commission:

CHRC File No. 20230074 – Aaruni Abhishek v. TD Bank

I trusted that the federal human rights body would investigate.

But as of 2025:

- the case remains unassigned
- no investigator has been appointed
- no timeline has been provided
- and no steps have been taken toward resolution

Justice delayed became justice denied.

Indicators of intention

Aaruni's intention to blow the whistle is evident through multiple actions. He wrote a detailed public article recounting the breach and the retaliation he faced. He filed a

complaint with the Canadian Human Rights Commission in 2023 under File No. 20230074. He participated in mediation in 2024 and continues to publicly discuss the issue through LinkedIn and Medium. These steps show a pattern of intentional escalation after internal processes failed.

Potential next steps

Based on the available information, he may continue pursuing legal remedies, including wrongful dismissal or human rights litigation. He could cooperate with the ongoing breach investigation led by Levi and Korsinsky LLP. He might also provide information to journalists, regulators, or privacy-focused watchdogs as the matter evolves. Each of these steps would align with typical whistleblower progression once internal channels and early remedies have been exhausted.

Anonymous whistleblower linked to the Miles Guo scheme

Findings related to the organisation

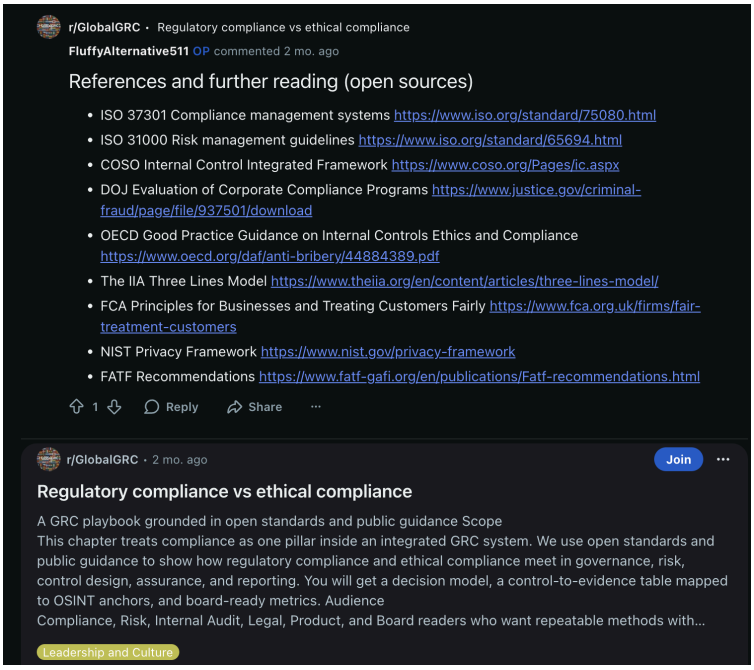
The *SEC litigation release* confirms that Ho Wan Kwok, also known as Miles Guo, conducted a large-scale fraudulent operation through unregistered securities offerings and misuse of investor funds. This is supported by the U S Department of Justice's press release documenting the one billion dollar fraud conspiracy and by multiple investigations reported by major outlets such as The Guardian and The New York Times.

How they were affected and motivated

Although the individual remains anonymous, their Reddit activity shows that they have been tracking high level financial misconduct cases. Their posts reference a one point two billion dollar crypto conspiracy in the UK and UAE, which aligns closely with the financial scale and structure of the Guo Wengui scheme. Their commentary indicates direct awareness of victims and compliance failures, which provides a clear motivation to warn others.

Indicators of intention for whistleblowing

The individual regularly posts case studies on major fraud events, including the Wirecard collapse, and shares governance and compliance frameworks like COSO, ISO standards, DOJ guidance, and OECD anti bribery materials. This pattern shows an active interest in exposing misconduct and educating others about how financial fraud is uncovered.



Potential next steps the individual may take

They may continue sharing anonymised insights through Reddit, direct readers toward official filings such as the SEC litigation release, or contact journalists and regulators through secure channels. Their focus on compliance tools and whistleblower pathways suggests they could submit information to enforcement agencies or assist other victims in doing so.

---

3. Conclusion

The investigation identified clear and consistent evidence of whistleblowing behaviour across the examined cases. Although each individual operated in a different sector and under different pressures, the same pattern emerged repeatedly: exposure to organizational misconduct, personal or professional harm following internal reporting, and a shift toward seeking external channels for disclosure.

Dr Christopher Day's case showed how systemic issues in the NHS can push individuals toward public reporting when internal processes fail. Aaruni Abhishek's experience reflected the risks faced by employees who uncover privacy and security breaches inside large financial institutions, especially when retaliation disrupts their career and personal stability. The anonymous compliance professional demonstrated how individuals with industry expertise may attempt to report large-scale fraud while maintaining anonymity for safety.

Across all cases, the supporting evidence from legal documents, regulatory findings, and media coverage strengthened the credibility of the individuals' claims. The behaviours observed on forums and social platforms further reinforced their intent to report wrongdoing, seek guidance, or warn others.

Overall, the findings confirm that OSINT can reliably reveal early indicators of whistleblowing activity, highlight organizational patterns of misconduct, and map the motivations that push individuals from internal reporting to external exposure.

---

4. References

2.1

https://www.sciencedirect.com/science/article/abs/pii/S0022103113001352

https://journals.sagepub.com/doi/10.1177/27000710241257432

2.2

https://blog.falcony.io/en/6-common-whistleblowing-cases-in-the-mining-and-extraction-industry

https://www.researchgate.net/publication/371804573_Whistleblowing_Measures_and_Its_Implications_in_the_Nigerian_Extractive_Industry

https://www.whistleblowers.org/oil-gas-case-studies/

https://www.ey.com/en_gl/insights/forensic-integrity-services/why-trust-is-essential-for-whistleblowing-programs-to-be-effective

2.4

https://www.linkedin.com/posts/aaruniabhishek_privacyrights-whistleblowerprotection-accountability-activity-7378682595594682368-0qB_?utm_source=share&utm_medium=member_desktop&rcm=ACoAAEMHdXUB34fPrSWumJo_WrQIUoMN3yHUqMU

https://theconcernedbird.substack.com/p/elon-musks-and-xs-role-in-2024-election

https://www.linkedin.com/posts/emmawalkerceo_whistleblowinguk-whistleblower-worldwhistleblowingday-activity-7342945339156422656-t8I3?utm_source=share&utm_medium=member_desktop&rcm=ACoAAEMHdXUB34fPrSWumJo_WrQIUoMN3yHUqMU

https://www.linkedin.com/posts/georgina-halford-hall_officeofthewhistleblower-dutyofcandour-activity-7317982355065860096-2IAD?utm_source=share&utm_medium=member_desktop&rcm=ACoAAEMHdXUB34fPrSWumJo_WrQIUoMN3yHUqMU

https://whistleblowersblog.org/government-whistleblowers/fema-whistleblowers-placed-on-indefinite-leave-after-the-katrina-declaration/

https://www.linkedin.com/posts/dr-chris-day-798790177_my-name-is-dr-chris-day-i-have-been-fighting-activity-7290068238015582209-dtVy?utm_source=share&utm_medium=member_desktop&rcm=ACoAAEMHdXUB34fPrSWumJo_WrQIUoMN3yHUqMU

2.5

https://www.reddit.com/r/Whistleblowers/comments/1itvkyk/elon_musk_is_faking_doge_results_to_hide_his/
https://www.reddit.com/r/japanlife/comments/1h3zk0g/fired_as_employee_after_catching_company_doing/

https://www.glassdoor.com/Community/the-worklife-bowl/i-have-a-problem-that-will-almost-certainlt-result-in-me-being-fired-the-company-i-work-for-is-using-data-aquired-under-license

https://www.reddit.com/r/TOR/comments/1fpoi9s/need_to_keep_whistleblower_complaint_anonymous/

https://www.reddit.com/r/TOR/comments/cl4t24/tor_for_whistleblowing/

2.6

https://www.reddit.com/r/employmenttribunal/comments/1kmqwx9/ive_created_a_community_for_whistleblowers/

https://www.reddit.com/r/Journalism/comments/1nk697j/how_to_send_a_tiparea_of_focus_to_anyone_in/

https://forum.torproject.org/t/what-will-a-forensic-computer-audit-reveal/13228

https://www.reddit.com/r/onions/comments/aytgcp/never_used_tor_before_but_i_want_to_search/

https://forum.torproject.org/t/anonymity-with-respect-to-uploading-files-via-tor/13791

2.7

https://assets.publishing.service.gov.uk/media/68a44ad1a66f515db69343f7/Dr_Christopher_Day_v_Lewisham_and_Greenwich_NHS_Trust__2025__EAT_123.pdf

https://www.theguardian.com/society/2018/oct/02/nhs-whistleblowing-protection-tribunal-junior-doctors

https://www.aaruniglobal.com/post/canada-s-whistleblowing-dilemma-an-editorial-on-the-implications-of-the-aaruni-abhishek-vs-td-case

https://hrlawcanada.com/2024/07/ontario-court-orders-td-bank-to-produce-unredacted-complaints-investigation-documents-in-wrongful-dismissal-case/

https://www.linkedin.com/posts/aaruniabhishek_whistleblower-privacybreach-datasecurity-activity-7339606408281133056-o5nb?utm_source=share&utm_medium=member_desktop&rcm=ACoAAEMHdXUB34fPrSWumJo_WrQIUoMN3yHUqMU

https://www.reddit.com/user/FluffyAlternative511/

https://www.justice.gov/usao-sdny/pr/ho-wan-kwok-aka-miles-guo-arrested-orchestrating-over-1-billion-dollar-fraud-conspiracy
https://www.theguardian.com/world/article/2024/jul/16/guo-wengui-fraud-trial

https://www.nytimes.com/2018/01/10/magazine/the-mystery-of-the-exiled-billionaire-whistleblower.html#

2.8
https://www.computerweekly.com/news/366627212/NHS-trust-accused-of-at-best-cavalier-at-worst-deceitful-behaviour-after-deleting-emails

https://fox40.com/business/press-releases/accesswire/981675/levi-korsinsky-llp-investigates-td-bank-data-breach/

https://www.linkedin.com/pulse/canadian-stranded-abroad-when-system-fails-its-own-aaruni-abhishek-jkntc/

https://www.sec.gov/enforcement-litigation/litigation-releases/lr-25668
