BULL BITCOIN FRANCE

operated by Leonod SARL
15 Place Jules Ferry, 69006 Lyon | whistleblowing@leonod.fr

Anonymous Whistleblowing

A Practical Guide

How to submit a report while protecting your identity

1. About this guide

Leonod SARL (operating Bull Bitcoin France) is a PSAN registered with the AMF and a CASP applicant under MiCA. Its whistleblowing procedure accepts reports from employees, contractors, clients, and any third party who becomes aware of potential misconduct, AML/CFT violations, or breaches of applicable regulations.

Reports are sent to: **whistleblowing@leonod.fr**, managed by the Chief Compliance Officer.

Anonymous reports are explicitly accepted, provided they are sufficiently substantiated: **they must describe the alleged facts, indicate the relevant time period, and identify (even approximately) the persons or functions involved**.

> **Purpose of this guide**
> This guide walks you through the technical steps to submit a report without revealing your identity: downloading Tor Browser, creating a disposable email address, and general best practices for protecting yourself before, during, and after reporting.

2. Step 1 — Download and use Tor Browser

Tor (The Onion Router) routes your internet traffic through a worldwide network of volunteer relays, hiding your IP address and making it very difficult for anyone to trace your connection back to your physical location or device. It is free, open-source, and legal in most countries.

2.1 Download Tor Browser

1. Go to the official Tor Project website: torproject.org
2. Click Download Tor Browser and select your operating system (Windows, macOS, Linux, or Android).
3. Before installing, verify the cryptographic signature of the installer — instructions are on the download page.
4. Open Tor Browser and click Connect. Wait for it to establish a circuit.

> **Warning — Download only from torproject.org**
> Never download Tor from third-party mirror sites or browser extensions claiming to provide Tor functionality — they may be compromised or monitored.

2.2 What Tor protects — and what it does not

Tor PROTECTS against…	Tor does NOT protect against…
Your IP address being seen by visited sites	The content you write in a report
Your approximate geographic location	Metadata embedded in attached files
Your ISP seeing which sites you visit	Logging into personal accounts during the same session
Network-level traffic analysis	Malware or keyloggers already on your device

2.3 Best practices inside Tor Browser

- Do not maximise the Tor Browser window — window size can be used as a browser fingerprint.
- Do not install add-ons or plugins inside Tor Browser.
- Do not open downloaded documents while still connected to Tor — open them offline.
- Do not log into any personal accounts (Google, social media, etc.) during the same Tor session.
- If concerned about network monitoring at home, use public Wi-Fi (library, café) instead.

3. Step 2 — Create an anonymous email address

While inside Tor Browser, create a disposable email address with no link to your real identity. Never use your work or personal email to submit a report.

3.1 Recommended services

Service	URL	Notes
Proton Mail	proton.me	Free, end-to-end encrypted, works on Tor. Best for receiving follow-up questions.
Guerrilla Mail	guerrillamail.com	Instant inbox, no sign-up. Use if you do not need replies.
Temp Mail	temp-mail.org	One-click disposable address. Simple and fast.

3.2 Creating a Guerrilla Mail address (fastest — no registration)

5. Inside Tor Browser, go to guerrillamail.com.
6. A random address is generated automatically. Note it down before sending your report.
7. Emails received appear in real time in the browser window.
8. Do not close this tab until you have finished and read any reply from Leonod.

3.3 Creating a Proton Mail account (recommended for follow-up)

9. Inside Tor Browser, go to proton.me and click Create a free account.
10. Choose a username with no connection to your name, employer, or location.
11. Do not add a recovery email or phone number when prompted.
12. Use a strong, unique password not used anywhere else.
13. Note the address and password securely — Proton Mail cannot recover a lost password.

Which service should I use?

Use Guerrilla Mail to submit quickly with no follow-up. Use Proton Mail if you want to remain available to answer questions from the compliance team — this allows a more thorough investigation.

4. Step 3 — Write and send your report

Reporting address: **whistleblowing@leonod.fr**

Reports are received and handled by the Chief Compliance Officer of Leonod SARL in strict confidence.

4.1 What to include

Anonymous reports are only accepted if sufficiently substantiated. You do not need formal proof — a good-faith concern is enough. Include as much of the following as you can safely share:

- **Who:** Names, job titles, or descriptions of the individuals involved.
- **What:** A clear description of the suspected misconduct or violation.
- **When:** Dates or time periods, even approximate.
- **Where:** The business unit, system, or process involved.
- **Evidence:** Document references, transaction IDs, or communications — only what you can share safely.

4.2 What NOT to include

- Your real name or personal email — unless you are choosing to identify yourself.
- Photos taken on a personal phone: they contain hidden EXIF metadata including GPS location, device model, and exact timestamp.
- Screenshots from internal systems that could uniquely identify your workstation, user account, or session.

Warning — Strip metadata from any files you attach

Documents, images, and PDFs often contain hidden metadata: author name, edit history, GPS coordinates, device identifiers.

Windows: right-click the file → Properties → Details → Remove Properties and Personal Information.

macOS: use Preview or install ExifTool (free).

Linux / command line: `exiftool -all= file.pdf`

5. Protecting your identity — general guidelines

5.1 Before you act

- Do not research this topic from a work computer or on your employer's Wi-Fi — IT systems often log every URL visited.
- Do not tell colleagues you plan to report, even those you trust fully.
- Consider whether the facts you know are uniquely yours. If only two or three people have access to certain information, reporting it may implicitly identify you even without your name.

5.2 Device security

- Use a personal device rather than a work device.
- If using a personal laptop, use a private/incognito profile that does not sync to cloud accounts.
- Disable location services before starting a Tor session.
- For maximum anonymity, consider Tails OS — a live OS that boots from a USB stick, leaves no trace on the host computer, and routes all traffic through Tor automatically.

5.3 Network security

- Avoid submitting from home broadband: your ISP can see that you connected to the Tor network, even if it cannot see what you sent.
- A public Wi-Fi network (library, café) adds a useful additional layer of separation.
- If you must use home broadband, consider connecting through a VPN before Tor (VPN → Tor). Choose a provider with a verified no-logs policy outside EU jurisdiction.

5.4 After sending your report

- Close the Guerrilla Mail tab or log out of Proton Mail immediately after finishing.
- Clear Tor Browser data: Settings → Privacy and Security → Clear Browsing Data.
- If you used Tails, simply shut down — all data is erased automatically on shutdown.
- Do not discuss having submitted a report with anyone until an investigation is underway and you have legal advice.

6. Your legal protections

Even when reporting anonymously, you should know the strong protections French and EU law provide to identified whistleblowers:

Legal instrument	Key protection
Loi Sapin II (2016), as amended by Loi Waserman (2022)	Prohibits all forms of retaliation against good-faith reporters: dismissal, demotion, harassment, or any other adverse action.
Directive UE 2019/1937	Requires effective internal and external channels, and guarantees the confidentiality of your identity throughout the process.

French Criminal Code Art. 226-10	Deliberately false reports made in bad faith are a criminal offence. Good-faith reports — even if unverified — are fully protected.

If you believe you are facing retaliation, you may contact the **Défenseur des droits** at defenseurdesdroits.fr.

7. External reporting — AMF

You may also report directly to the Autorité des marchés financiers (AMF) at any time, independently of internal channels. The AMF accepts anonymous submissions.

Channel	Details
Secure online form	amf-france.org/en/forms-and-declarations/whistleblowing
Sealed postal mail	AMF — DCE / Service du lanceur d'alerte, 17 place de la Bourse, 75082 Paris Cedex 02. Mark envelope: Confidentiel – Signalement d'une alerte
By phone	Verbal report; AMF may record with consent or prepare a written transcript.
In person	Confidential meeting by appointment with the AMF whistleblowing unit.

8. Quick-reference checklist

Before you submit

- ☐ Using Tor Browser downloaded from torproject.org
- ☐ Using a personal device, not a work device
- ☐ Connected on public Wi-Fi or via VPN → Tor
- ☐ Created a disposable or Proton Mail address with no personal info
- ☐ Stripped metadata from any files to be attached
- ☐ Not logged into any personal accounts in this session
- ☐ Report contains: facts, time period, persons involved (even approx.)