How INTERPOL Finds and Tracks People: Red Notices, Diffusions, and Airport "Hits" Explained

By Friling Law PLLC – Interpol defence and representation lawyers

INTERPOL is not a global police force, and it doesn't have the power to arrest anyone. It's a coordination platform—an international system that lets member countries share data and request cooperation through standardized alerts and connected databases.

So when someone says, "INTERPOL is looking for me," it usually means something more specific and less dramatic. In practice, it's typically one (or more) of the following:

- **A Notice** recorded in INTERPOL's systems (most commonly a Red Notice);
- **A Diffusion** circulated directly by a member country to others; and/or
- **A database hit**, especially in the SLTD (Stolen and Lost Travel Documents) database, triggered when a passport or ID is checked at a border or by law enforcement.

The distinction matters, because each of these operates under different rules, review processes, and remedies—even though they often get blurred together in real life.

1) The main alert products used to seek people

A. Red Notices

A Red Notice is essentially a global "wanted" alert: it asks law enforcement around the world to locate and provisionally detain someone, usually pending extradition or similar legal action. It's always based on an arrest warrant or judicial decision issued in the requesting country. Each member country then decides, under its own laws, whether to make an arrest.

Two important points for understanding real-world risk:

- A Red Notice is **not** an international arrest warrant. INTERPOL explicitly clarifies this.
- Most Red Notices are **not public**. INTERPOL notes that the majority are "restricted to law enforcement use only." (www.interpol.int)

B. Diffusions

A Diffusion is a more targeted cooperation request sent directly by a member country's National Central Bureau (NCB) to some—or all—other member countries. Diffusions use the same color-coded system as Notices (red, blue, yellow, etc.) and must follow INTERPOL rules.

In practice, Diffusions can spread quickly and have effects similar to Red Notices—especially during border checks or law-enforcement encounters—even though they usually aren't public-facing.

2) The channels that move INTERPOL alerts across borders

A. I-24/7 – INTERPOL's secure global network

INTERPOL links member countries through I-24/7, a secure communications system. It allows countries to contact each other and the General Secretariat, access INTERPOL services, and tap into real-time databases—even from remote or frontline locations.

B. INTERPOL databases – where most "hits" happen

Most of the high-impact alerts come not from someone reading a Red Notice but from a database match during routine identity or document checks. A prime example is:

- **SLTD (Stolen and Lost Travel Documents):** tracks passports and IDs that are stolen, lost, revoked, invalid, or even blank and stolen. Law enforcement can check document validity in seconds.

C. Border management – frontline access

Border officers can access INTERPOL databases directly, whether at fixed checkpoints or using mobile devices, allowing real-time identity checks for travelers.

D. Command and Coordination Centre (CCC) – 24/7 support

INTERPOL's CCC operates around the clock from multiple regions, helping national police coordinate urgent cross-border matters, such as locating fugitives or verifying identities.

E. Biometrics – fingerprints and facial recognition

The Biometric Hub lets member countries upload fingerprints and facial images, which are then checked against INTERPOL's biometric databases for potential matches.

F. Specialized Notices – UN sanctions and asset tracing

INTERPOL also issues targeted alerts for complex cases:

- **UN Security Council Special Notices:** flag individuals or entities subject to UN sanctions.
- **Silver Notice (assets):** launched in January 2025, this pilot helps countries track information on criminal assets like real estate, vehicles, bank accounts, and businesses.

3) Where and how INTERPOL-related alerts surface: airports, hotels, rentals, and other touchpoints

A. Airports – the highest-risk "hit" environment

1. **Government screening at borders and immigration controls**

   When traveling, whether at departure, transit, or arrival, border and immigration officers often check travelers against INTERPOL-linked databases—especially the SLTD (Stolen and Lost Travel Documents). INTERPOL notes that document validity can be verified in seconds.

If there's a "hit," the typical next steps may include:

- Referral to secondary screening
- Confirmatory document or identity checks
- Coordination with local law enforcement or the country's National Central Bureau (NCB)

2. **Airline and travel-sector screening**

   Through **I-Checkit**, accredited private-sector partners (like airlines) can submit data for screening against certain INTERPOL databases. Importantly, the airline does **not** get full access to INTERPOL databases, nor does INTERPOL access the airline's internal systems. A match simply triggers review by the authorities under the program rules—it doesn't mean the airline "has your file."

B. Hotels – usually indirect exposure

Most hotels are not directly connected to INTERPOL. Risk usually comes through local guest-registration or reporting rules, which vary by country and may make identity data accessible to authorities.

Where hotels do participate in screening programs, it is still via the controlled I-Checkit "push" model—hotels transmit data, but do not have direct access to INTERPOL systems.

C. Car rentals – rarely a direct INTERPOL point

Rental counters usually don't screen against INTERPOL. Risk arises mainly through:

- Domestic ID or fraud checks if documents look suspicious;
- Later law-enforcement contact (traffic stops, accidents, roadside checks), where officers may query INTERPOL-linked databases via I-24/7

D. Other locations where exposure can occur

- Land borders and seaports: these checkpoints can access INTERPOL databases directly
- Any official identity-check environment: even if arrests or detentions happen under local law, INTERPOL connectivity can flag individuals for additional review

4) Safeguards and legal review: neutrality and remedies

A. The Article 3 neutrality rule

INTERPOL operates under a strict neutrality principle: it cannot get involved in activities of a political, military, religious, or racial nature. This rule is central to how the organization handles alerts, notices, and any requests for international police cooperation.

B. The CCF – managing access, correction, and deletion

The **Commission for the Control of INTERPOL's Files (CCF)** is an independent body that makes sure INTERPOL's data rules are followed. It handles individual requests to:

- Access data
- Correct inaccuracies
- Delete information from INTERPOL's Information System

INTERPOL also provides guidance on how long these requests typically take, with timelines for access and correction/deletion decisions—though actual processing depends on whether the request is admissible and follows proper procedure.

5) Practice checklist and risk matrix

First 48 hours: practitioner checklist

- Identify the product/channel: **Red Notice** vs **Diffusion** vs **SLTD hit** vs **UN Special Notice** vs **Silver Notice**.
- Map exposure points: upcoming travel, transit hubs, border crossings, and other high-friction identity checkpoints.
- Confirm the domestic legal engine: whether a national warrant/court order exists and how destination/transit jurisdictions treat Red Notices/Diffusions under local law. Preserve evidence: incident reports, boarding denials, secondary screening notes, document copies, and any law-enforcement communications.
- Evaluate CCF strategy where data appears inaccurate, abusive, or Article 3-implicated.

Quick risk matrix

Channel / product	Where it most commonly surfaces	Typical immediate consequence	Primary response focus
SLTD database hit	Airports/borders/frontline checks (interpol.int)	Secondary screening; document verification/seizure	Document provenance; identity resolution; remediation plan
Red Notice	Border/police encounters; domestic lookout lists (interpol.int)	Possible detention (jurisdiction-dependent)	Extradition posture; warrant validity; parallel risk controls
Diffusion	NCB-to-NCB circulation; similar touchpoints (interpol.int)	Similar disruption/detention risk	Rapid fact development; targeted jurisdiction analysis
I-Checkit screening	Pre-travel/private-sector push screening (interpol.int)	Authority notification; downstream screening	Clarify dataset/trigger; manage travel and compliance risk

UN Special Notice	Sanctions-related enforcement touchpoints (interpol.int)	Travel restrictions/compliance escalation	Sanctions scope; legal exposure; due diligence controls
Silver Notice	Asset tracing/intelligence exchange (interpol.int)	Requests for asset information; investigative pressure	Asset mapping; cross-border counsel coordination

FAQ: INTERPOL Red Notices, Diffusions, and Real-World Screening

1) Is an INTERPOL Red Notice the same as an international arrest warrant?

No. A Red Notice is an alert asking authorities worldwide to locate and provisionally arrest someone pending extradition or similar legal proceedings. Whether someone is actually arrested depends entirely on the local laws and procedures of the country where they are encountered.

2) What's the difference between a Notice and a Diffusion?

A Notice is a standardized **INTERPOL** alert processed through official INTERPOL channels. A **Diffusion** is a request sent by a member country (usually via its National Central Bureau) to other countries. Diffusions are often faster and less formal but can have similar real-world consequences.

3) Can a Red Notice or Diffusion stop me at the airport?

Yes. Airports are common places where issues appear because border and immigration authorities screen IDs and travel documents. If there's a match, travelers may be sent to secondary inspection, questioned, delayed, denied boarding or entry, or even detained—depending on local law.

4) What is SLTD, and why does it matter?

SLTD stands for Stolen and Lost Travel Documents. It's INTERPOL's database of passports and IDs that have been reported stolen, lost, revoked, invalid, or blank. Matching against SLTD can trigger immediate scrutiny at borders and airports.

5) If my name isn't on INTERPOL's website, does that mean I'm not flagged?

Not necessarily. Many notices are restricted and not publicly available. Diffusions usually aren't public either. So just because you don't see your name online doesn't mean there's no alert.

6) Do hotels see INTERPOL alerts when I check in?

Usually not. Hotels typically don't have direct access to INTERPOL systems. Any exposure is usually indirect, via local guest-registration rules or local authorities. Some controlled programs allow limited private-sector screening, but it's not the same as direct database access.

7) Do car rental companies check INTERPOL?

Usually no. Rental counters aren't typical screening points. Exposure is more likely through domestic ID verification rules or later law-enforcement encounters, like traffic stops or accidents.

8) Can INTERPOL remove or delete a Red Notice?

Not informally. There's a formal process: individuals must go through INTERPOL's independent review body, the CCF, which handles access, correction, or deletion requests, provided admissibility requirements are met.

9) What other types of INTERPOL alerts exist besides Red Notices?

INTERPOL issues various alerts for different purposes, including locating missing persons or gathering intelligence. There are also specialized products, like UN sanctions notices or pilot asset-tracing notices. Practical risk depends on the alert type and how national authorities act on it.

10) What should I do if I think I'm flagged by INTERPOL?

Identify the type of alert: Red Notice, Diffusion, or database hit.

- Document the incident: when, where, and how it occurred.
- Seek qualified counsel to assess your risk: consider jurisdiction-specific arrest/extradition exposure and whether a formal data challenge through the CCF is appropriate.

11) Can I travel internationally if there's an INTERPOL alert against me?

It depends. Risk varies by alert type, the underlying legal basis (warrant/order), the countries on your itinerary (including transit points), and how those countries treat INTERPOL alerts under their domestic law.

12) Does INTERPOL investigate crimes or make arrests?

No. INTERPOL does not have arrest powers. It facilitates cross-border cooperation and information sharing. Investigations and arrests are handled by national authorities under their own laws.

Conclusion

INTERPOL itself does not arrest anyone. Instead, it acts as a hub for international police cooperation, circulating alerts—like Red Notices and Diffusions—and maintaining databases that can trigger "hits" at borders and airports, especially during passport or ID checks (notably through the SLTD database). This guide has explained how alerts and data flow through INTERPOL's I-24/7 network and databases, why the most immediate consequences usually happen at airports and border crossings, and why hotels and car rentals generally only create indirect risk through local reporting or later law-enforcement encounters. Finally, it highlighted key safeguards—particularly Article 3's neutrality rule—and the main procedural remedy for affected individuals: submitting access, correction, or deletion requests to the CCF when data appears inaccurate, abusive, or otherwise inconsistent with INTERPOL's rules.