INTERPOL

INTERPOL MEMBER COUNTRIES

I-Checkit

FREQUENTLY ASKED QUESTIONS

Q1. WHAT IS I-CHECKIT?

I-Checkit is a screening service that complements and enhances existing national border security systems. It allows partners in the private sector to conduct advance checks on identification documents against INTERPOL's Stolen and Lost Travel Documents (SLTD) database.

Q2. WHO CAN USE I-CHECKIT?

I-Checkit is currently used by airlines and cruise lines. Further development areas include the banking, financial and hospitality sectors.

All partners are carefully selected in compliance with INTERPOL's rules and regulations and must be endorsed by the INTERPOL National Central Bureau (NCB) in the country where they are registered.

Q3. WHO ARE I-CHECKIT'S MAIN STAKEHOLDERS AND HOW DO THEY BENEFIT FROM THE SERVICE?

1. Border police, customs & immigration, Ministries of Interior, intelligence agencies and INTERPOL NCBs use I-Checkit as an additional screening capability to strengthen border security;
2. Technology service providers such as those providing document verification solutions may choose to integrate I-Checkit to complement their service offering;
3. Professional associations including the International Air Travel Association (IATA), World Travel and Tourism Council (WTTC) and World Economic Forum (WEF) have launched initiatives aimed at enhancing security and improving passenger travel and see I-Checkit as a recognized platform to test and support their initiatives;
4. Regulatory bodies such as the International Civil Aviation Organization (ICAO), INTERNATIONAL MARITIME ORGANIZATION (IMO), AND EUROPEAN BORDER AND COAST GUARD AGENCY (FRONTEX) CONSIDER I-CHECKIT AS AN INNOVATIVE SOLUTION TO REINFORCE THEIR INTERNATIONAL STANDARDS AND REGULATIONS.

Q4. WHAT INFORMATION IS NEEDED FOR AN I-CHECKIT SCREENING?

The inclusion of nominal data is not necessary for I-Checkit screenings. Only the travel document number, country of issuance and document type (i.e. passport, ID card or visa) are screened against the SLTD database. These elements are not considered nominal data under INTERPOL's legal framework and are used in accordance with INTERPOL's Rules on the Processing of Data (RPD).

Q5. WHAT ARE THE BENEFITS TO MEMBER COUNTRIES?

- By extending screening capabilities to the private sector, an additional layer of security is provided to member countries, complementary to integrated national border security infrastructure;
- It is a risk mitigation tool for those countries without integrated border capabilities;
- As a pre-travel screening capability, it allows for advance detection and deterrence of threats and facilitates law enforcement action;
- It provides additional security to airlines and is aligned with UNSCR 2309 to

ensure the safety of global air services and prevent potential terrorist attacks to civil aviation.

Q6. ARE PRIVATE COMPANIES GRANTED DIRECT ACCESS TO INTERPOL'S DATABASES AND VICE VERSA?

No. Private companies do not have direct access to INTERPOL's databases, nor does INTERPOL have access to private companies' databases. Instead, a 'push' system is implemented, in which required data is extracted and sent via the I-Checkit solution for screening. It is important to note that private entities cannot search or modify the information held in the SLTD database.

Q7. WHAT KIND OF RESPONSE IS SENT TO PRIVATE ENTITIES?

In case of a match, or 'hit', on a travel document issued by a country who opted for the visible I-Checkit mode, the private entity will receive a notification message that includes:

- Travel document information: the type of document, the document number and issuing country;
- The passenger's itinerary information: extracted from the private entity's check-in system (if applicable);
- Recommendations on how to follow up on the hit.

In case of an SLTD hit on a travel document issued by a country who opted for the non-visible I-Checkit mode, the private entity will not receive a hit notification message.

For more information on participation modes, see question 11.

Q8. HOW LONG DOES THE SCREENING PROCESS TAKE?

Although processing times can vary depending on network connectivity, screenings are normally processed in **30 milliseconds.**

Q9. WHAT IS THE FINANCIAL FRAMEWORK BEHIND I-CHECKIT?

As a not-for-profit organization, INTERPOL aims to provide policing capabilities that benefit the international community and, as a result, I-Checkit is based on a cost recovery model.

Once the early testing phase has been completed, private entities are charged an annual subscription fee to access the I-Checkit solution. The fee covers the cost incurred by INTERPOL to deliver the service.

Proceeds generated by I-Checkit are reinvested into INTERPOL's activities that support the key areas impacted by increased screenings. That includes teams involved in hit follow-up activities, enhancing database quality management, I-Checkit training sessions and the actual delivery and continuous improvement of the service. It is also envisaged that part of the subscription fees may be used to provide operational and material support to highly impacted NCBs.

OPERATIONAL CONSIDERATIONS

Q10. HAVE ANY REFERENCE MATERIALS BEEN DEVELOPED TO SUPPORT THE OPERATIONS OF I-CHECKIT?

INTERPOL has developed Standard Operating Procedures and Policies (SOPPs) which describe the roles and responsibilities of I-Checkit stakeholders' business processes and rules and the expected service delivery levels. Distinct SOPPs have been developed for both the aviation and maritime sectors and can be requested via the following email I-Checkit@interpol.int .

Q11. CAN MEMBER COUNTRIES CONTROL HOW THEIR DATA IS USED?

Yes. When deciding whether they will participate in I-Checkit, member countries are presented with three alternative participation modes:

1. Opt-out: Screenings cannot be performed by the private entity against the country's data in the SLTD;
2. Opt-in under 'visible' mode: Screenings can be performed by the private entity and hit notifications will be automatically sent to the private entity's security team;
3. Opt-in under 'non-visible' or 'blind' mode: Screenings can be performed by the private entity, however, no notifications are sent to the entity's security team. It is at the discretion of the concerned NCBs to choose whether information is shared.

184 INTERPOL member countries currently participate in the programme either under 'visible' or 'non-visible' mode, with others reviewing their national legislations with a view to joining at a later stage.

Q12. IS THE CONNECTION TO INTERPOL'S DATABASES SECURE?

Yes. Access is facilitated through a secure connection via the I-Checkit screening solution, allowing the user's system to instantly transmit data for screening against INTERPOL's databases via an encrypted VPN tunnel. This solution has proven to be as secure as INTERPOL's I-24/7 global police communications system. Additionally, the screening solution is hosted in INTERPOL's Secure Cloud.

Q13. HOW IS I-CHECKIT IMPLEMENTED?

The implementation process is comprised of three stages:

1. The pilot phase, which includes the following key steps:
   - Non-disclosure agreement
   - Preparation workshop
   - Scoping document
   - Agreement signature
   - Endorsement from the NCB where the company is registered and, in the case of carriers, the NCB of departure
   - Three-month trial phase to test the solution in a real environment

2. Pilot review to ascertain whether I-Checkit is suited to the company's needs
3. Full rollout

Q14. WHAT ROLES DO NCBS PLAY IN I-CHECKIT?

The **NCB of Registration** (where the private entity's headquarters is based)

- Must endorse the private entity before I-Checkit is implemented;
- May choose to take on a leading role to follow up on a hit, together with the private entity's contact point and the NCB who owns the data.

NCB Data Owner (NCB of the country that owns the SLTD data)

- Is the central point of contact for both the verification and confirmation of positive search results;
- Is the NCB which will follow and support all aspects of the travel document verification process.

NCB of Departure (NCB of the country of port/airport of embarkation or turnaround/transit port/airport)

- The NCB of the country where the passenger is located or presenting a travel document recorded in INTERPOL's databases;
- As the local link to INTERPOL's global network, this NCB in a unique position to liaise with the company's security representatives and national law enforcement authorities to locate and interdict the document holder or passenger, when he/she moves to/from/within their territory in order to verify the authenticity of the travel document prior to the passenger's departure.

NCB of Arrival and/or Transit (NCB of the country of port/airport of disembarkation or turnaround/transit port/airport)

- The NCB of the arrival country and NCB of the transit country also play a role in the resolution process in the event that the passenger was not detected or intercepted by the country of departure.
- Will be notified by INTERPOL through the I-Checkit service of positive search results when their country is impacted by the flight/cruise itinerary.
- Should ensure communication with NCB Data Owner / Source during the follow-up process.

Q15. WHAT IS THE PROCESS FOR NCBS ONCE A 'HIT' IS GENERATED?

Upon reception of a hit, it is recommended that the **NCB Data Owner** confirm the match by sending the following information to INTERPOL's Command and Coordination as well as the **NCB of Departure**:

- Full personal identity of the legitimate bearer of the document;
- Dates of issuance and expiration of the travel document;
- Identification material of the legitimate bearer if available (photo, fingerprints), in accordance with national data protection rules and regulations;
- Operating instructions regarding the passenger's detention on the day of embarkation (if applicable).

The **NCB of Departure** is then encouraged to share this information with the immigration authorities at the airport/port on the day of embarkation to facilitate verification of the travel document / bearer. It is important to note that a confirmed 'hit' points to the risk of a stolen identity in the hands of an individual with criminal intent and/or an individual wanted on criminal charges and should be mitigated accordingly, as per existing national procedures.

The INTERPOL Command and Coordination Centre (CCC) will remain available to support the communication channels with all involved parties.

LEGAL CONSIDERATIONS

Q16. IS I-CHECKIT COMPATIBLE WITH INTERPOL'S MANDATE?

I-Checkit is a vital component of INTERPOL's Strategic Framework (Goal 2 and objective 2.4) and is aligned with the Organization's Global Counter-Terrorism Strategy under the 'Travel/Mobility' action stream, key Objective 2.7 'Develop and Implement Private-Public Screening Solutions'.

Q17. INTERPOL HAS PUT IN PLACE A COMPREHENSIVE LEGAL FRAMEWORK TO ENSURE THE SERVICE'S FULL COMPLIANCE. THE FRAMEWORK INCLUDES THE FOLLOWING COMPONENTS:

- INTERPOL's Constitution
- INTERPOL's Rules on the Processing of Data (RPD)
- Exchange of information with private companies
- Data retention
- INTERPOL's Financial Regulations, which allows IPSG to charge a fee to recover costs borne by the Organization in delivering the service;
- National and international law (service subject to national legislation in member countries, any countries' participation must be in accordance with their own national laws, approval by national data protection authority when necessary);
- Contractual agreements with private companies (stipulates parameters by which companies must abide - no direct access to INTERPOL information system, no retention of any data obtained through I-Checkit, immediate deletion of all I-Checkit related data once flight / vessel has departed, binding obligation to establish a person's identity, informing passengers of use of their data);
- International data protection standards (overseen by the Commission for the Control of Files).

If you have any additional questions, please do not hesitate to contact the I-Checkit team at I-Checkit@interpol.int