# Veriff CrossLinks

veriff

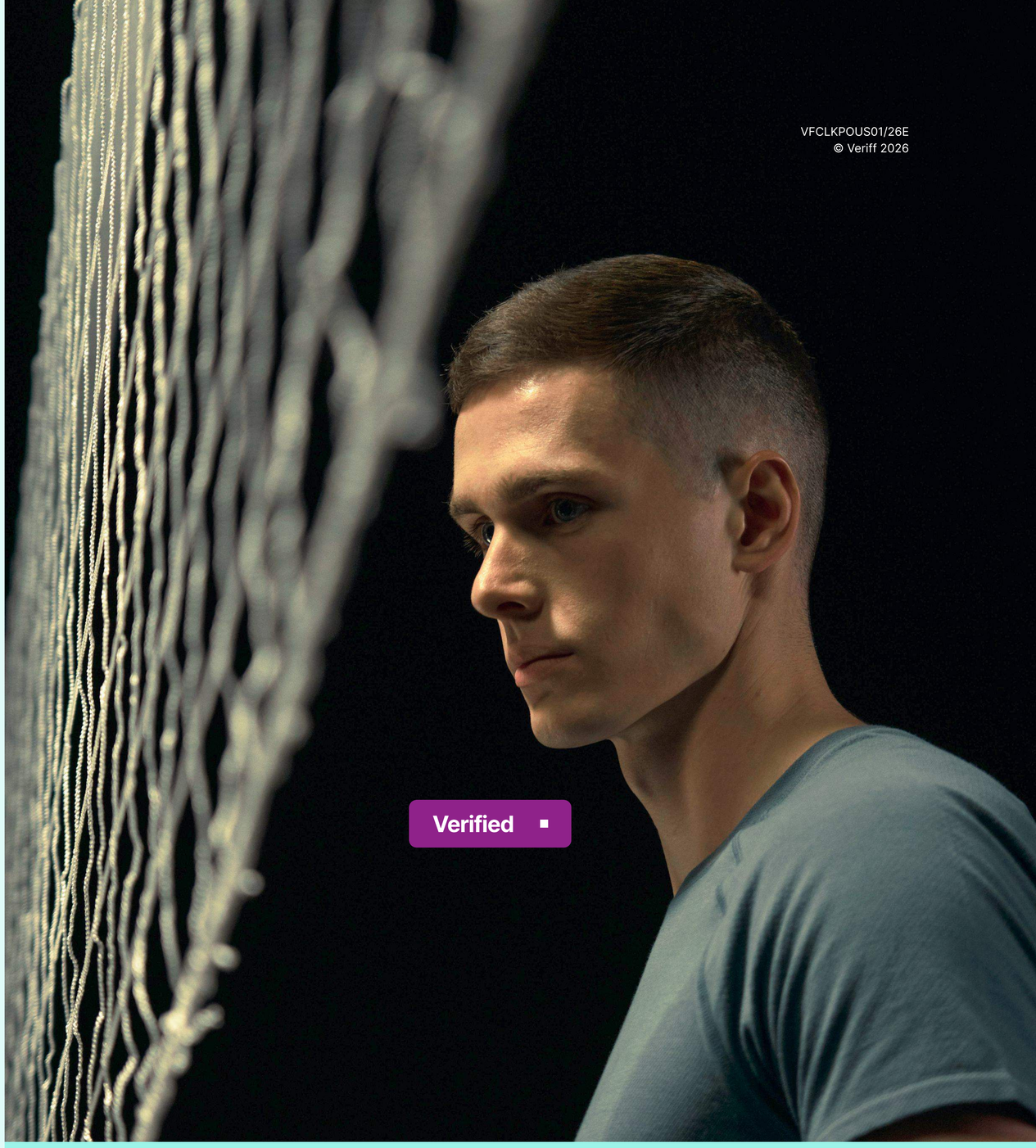
## Network-based fraud detection for trusted identity decisions

- Technical sheet

veriff

**Customer verification built for global businesses**
**veriff.com**

# Veriff CrossLinks: network-based fraud detection for trusted identity decisions




**Let’s talk about CrossLinks:**
**contact sales@veriff.com**

## Overview

In an increasingly sophisticated threat landscape, analyzing a single verification session in isolation is no longer enough to stop professional fraud rings. CrossLinks is Veriff’s advanced fraud detection capability, designed to uncover risk patterns that are not visible when evaluating individual sessions alone. By intelligently linking verification sessions that share meaningful similarities—such as device, network, document, or facial data—CrossLinks exposes repeat fraudsters, synthetic identities, multi-accounting, and coordinated fraud rings in real time.

Rather than treating each verification as a standalone event, CrossLinks provides a connected view of activity across sessions. This allows businesses to make more informed, data-driven decisions while maintaining a fast, seamless experience for genuine users.

## Why CrossLinks matters

Professional bad actors rarely stop at a single attempt; they scale their operations by reusing hardware, connectivity infrastructure, or modified documents. While an individual session might appear legitimate on the surface, its connection to a previously declined or suspicious attempt reveals the true underlying risk.

Without cross-session visibility, these sophisticated patterns can go undetected. CrossLinks transforms these repeated behaviors into your strongest defense, turning a fraudster’s footprint into a permanent red flag.

## Key benefits

1. **Stronger fraud detection:** Expose complex fraud rings by detecting clusters of accounts that appear unrelated but share a single device or biometric profile.
2. **Stop "serial" fraudsters:** Instantly flag individuals who attempt to onboard with a new identity or stolen document after a previous rejection.
3. **Real-time risk signals:** Receive high-fidelity alerts as they happen, enabling your team to automate declines or trigger immediate escalations.
4. **Enhanced decisioning intelligence:** Risk labels provide immediate context on a user’s history across your ecosystem, focusing your manual review resources on the sessions with the highest risk indicators.
5. **Optimized user experience:** Sophisticated filtering ensures genuine users aren't incorrectly flagged by "noisy" matches, such as shared public Wi-Fi or common names.
6. **Privacy-centric protection:** CrossLinks leverages advanced embeddings and technical metadata to identify high-risk patterns without compromising PII (Personally Identifiable Information) security.

# How CrossLinks works

CrossLinks continuously monitors and analyzes incoming verification sessions, comparing them against historical data in real time. Rather than relying on simple one-to-one matches, the CrossLinks engine utilizes a multi-layered analysis to identify high-risk connections across multiple data dimensions, including document data, device fingerprints, behavioral signals, network indicators, and face embeddings.

To ensure accuracy and minimize false positives, cross-linking is performed across multiple layers simultaneously. This approach allows CrossLinks to distinguish between incidental similarities or "noisy" data – such as two strangers using the same public Wi-Fi network versus a fraudster using the same mobile device for 10 different identities.

The process in action:

- **Data capture:** As a user onboards, Veriff captures document data, device fingerprints, network signals, and biometric face embeddings.
- **Comparison engine:** The system automatically cross-references these data points against your existing session history to identify potential connections in real time.
- **Risk labeling:** When a meaningful connection is detected, CrossLinks is surfaced via a Risk Label attached to the session. Risk Labels are visible in Veriff Station and can also be delivered via webhooks, highlighting session-level information that may indicate elevated fraud risk—such as the linked user's name and previous verification dates. For example, if a fraudster was declined yesterday for submitting a fake passport and tries again today with a different name but the same smartphone, CrossLinks immediately flags the connection. This allows your team to trigger an automated decline or a manual fallback review, helping stop repeat fraud attempts before they escalate.

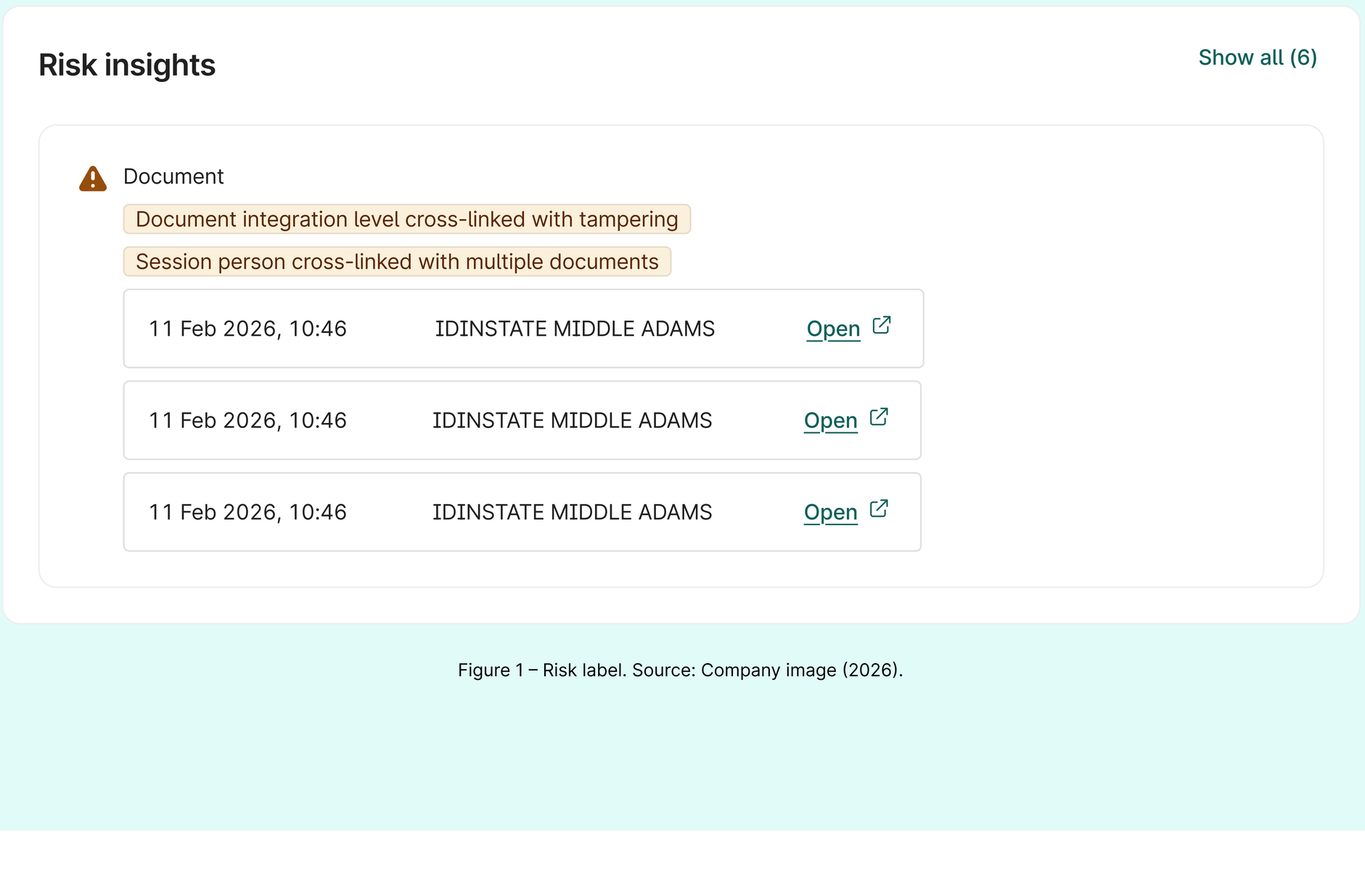



Figure 1 – Risk label. Source: Company image (2026).

# Levels of CrossLinks

## 1. CrossLinks (customer-specific)

This foundational layer operates exclusively within your own user base. It is designed to stop repeat offenders who cycle through identities to attack your platform specifically. By ensuring that a fraudster declined yesterday cannot return today under a new alias, you close the door on persistent threats.

Example: A user attempts to claim multiple "new user" bonuses by signing up with three different names. CrossLinks identifies that all attempts share the same device and facial biometrics, instantly blocking the bonus abuse.

## 2. Industry CrossLinks (the network effect)

Industry CrossLinks extend Veriff's cross-linking capabilities by applying the same detection logic across Veriff's network of customers within the same industry vertical.

Fraudsters rarely target just one organization. Instead, they launch repeated attacks across multiple companies within the same vertical. Industry CrossLinks addresses this challenge by creating a privacy-preserving "fraud consortium," where intelligence from previously detected fraud attempts is used to help protect other organizations within the same industry (such as fintech, mobility, or crypto).

Using privacy-first methods, Industry CrossLinks analyzes technical signals, document information, and face embeddings to determine whether an incoming session is linked to a session previously declined by another organization in the same industry. The session is flagged with a **"Session cross-linked across multiple clients"** risk label only when such a connection is identified.

Example: if a fraudster is detected and declined by one ride-sharing platform, that intelligence becomes immediately actionable across the industry network. When the same fraudster attempts to onboard with a competing delivery or mobility service, the session is flagged as a high-risk repeat offender.

Key benefits of Industry CrossLinks include:

- **Network effect protection:** stop fraudsters already identified by other organizations in your industry.
- **Early risk awareness:** gain visibility into emerging fraud patterns across the wider ecosystem.
- **Traffic quality insights:** even approved sessions may carry risk indicators that support internal risk scoring and decision-making

No personal data or customer identity is shared as part of Industry CrossLinks. Customers receive only a risk label indicating a cross-industry connection, without visibility into which organization detected the fraud or the outcome of that session. This allows you to benefit from the "community's" knowledge while preserving strict privacy boundaries.

## 3. Extended CrossLinks (the long-term view)

Standard CrossLinks typically monitors "live" session data (the most recent 3 months). However, sophisticated actors often wait for their trail to go "stale" before reappearing. Extended CrossLinks broadens this window to up to three years, including archived data. This prevents bad actors from "waiting out" detection and uncovers dormant fraud patterns that emerge over a longer time horizon.

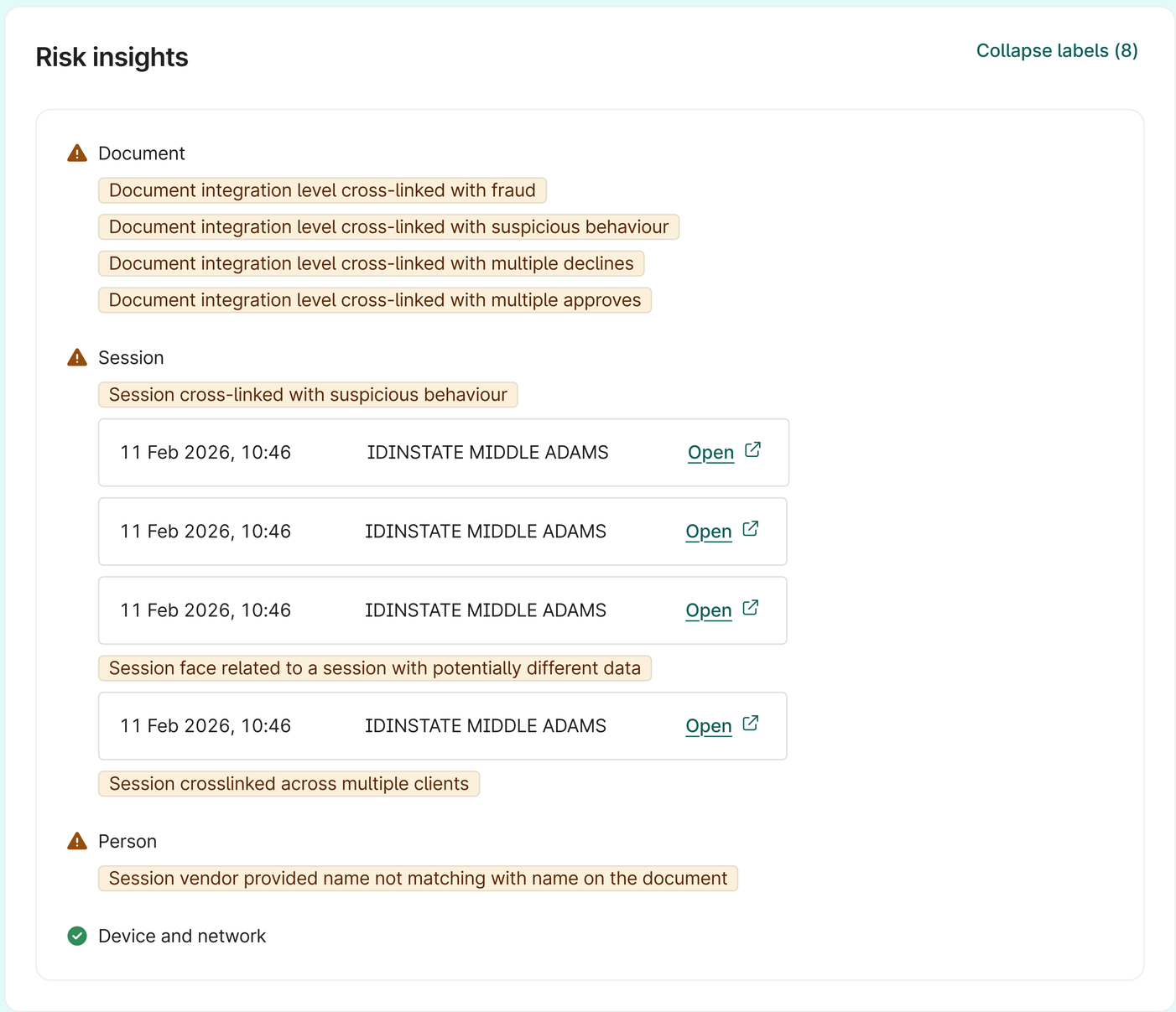



Figure 2 – Risk label example. Source: Company image (2026).

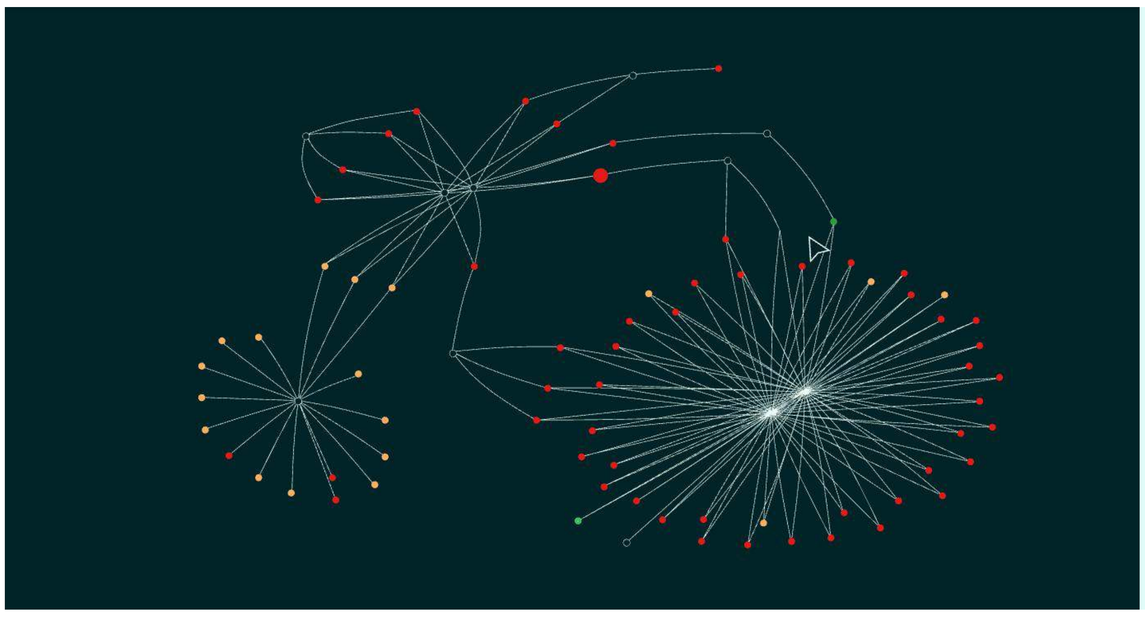
# Summary

CrossLinks is a foundational component of Veriff's fraud prevention technology—delivering smarter, context-driven risk detection through real-time session connectivity. By turning isolated data points into a connected intelligence network, Veriff empowers businesses to stay ahead of evolving threats while preserving user trust.

**Technical Specifications**

- **Integration:** supports both full auto and hybrid (auto+manual) flows.
- **Data Points:** includes device IDs, IP addresses, document numbers, and biometric face templates.
- **Visibility:** real-time risk labels delivered via API/Webhooks and Veriff Station.
- **Compliance:** fully compliant with data retention periods and global privacy standards.

| Feature | Network coverage | Data age | Key use case |
|---|---|---|---|
| **CrossLinks** | Single customer | Live (≈3 months) | Preventing multi-accounting, repeat fraud, and coordinated attacks |
| **Industry CrossLinks** | Industry network | Live (≈3 months) | Stopping industry-wide "hit and run" attacks. |
| **Extended CrossLinks** | Single customer | Up to 3 years | Detecting long-term patterns and patient fraud actors. |



## See CrossLinks in action! View the video:

Play now

VFCLKPOUS01/26E


Customer verification built for global businesses
veriff.com