sumsub

// FRAUD DEFENSE CHECKLIST

Below are some practical tips to improve your fraud defenses, no matter where you're based in the world.

Fraud Activity

With the right fraud response strategies in place, you can safeguard your business against both known and emerging threats.

- Create a fraud response plan with a structured protocol to swiftly tackle emerging risks, including clear lines of communication across departments.
- Leverage AI and machine learning for continuous transaction monitoring, enabling the detection of not just known patterns, but emerging threats through anomaly detection.
- Establish a Suspicious Transaction Reporting (STR) system that includes automated alerts for any unusual activity, ensuring accurate filings within regulatory deadlines and avoiding fines.
- Offer regular training to your employees on how to ensure compliance with local regulations and respond effectively.
- Conduct regular audits of your fraud prevention protocols to assess their effectiveness and identify gaps.
- Introduce geolocation monitoring to ensure transactions and logins align with customer activity, flagging anomalies for further review.
- Implement stringent user verification, business verification, AML checks, UBO identification, and verify the source of funds.

LEARN MORE ABOUT SUSPICIOUS ACTIVITY REPORTS →

Resource Accessibility

Strengthen your fraud prevention by enhancing resource accessibility and cybersecurity measures where possible.

- Improve access to secure and reliable internet connections to prevent downtime that fraudsters can exploit.
- Adopt stronger cybersecurity measures, including multi-factor authentication, firewalls, and encryption to safeguard your data, as well as regular vulnerability assessments to ensure defenses are always up to date.
- Tailor KYC/AML compliance practices to the specific risks and regulatory landscapes of the countries you operate in, considering the digital resource accessibility and fraud prevalence in those regions.
- Develop fraud prevention training to educate employees about detecting scams, with a particular focus on emerging fraud types such as synthetic identity fraud.
- Use AI-driven fraud detection tools to handle scaling transaction volumes without sacrificing security.
- Implement secure document storage and access control to minimize the risk of unauthorized data exposure.

LEARN MORE ABOUT BIOMETRIC AUTHENTICATION →

Government Internvention

Since government anti-fraud measures vary globally, here's what you can do to help bridge the gaps.

- Continuously monitor developments in AML/CFT regulations to ensure your business remains compliant across all jurisdictions.
- Establish clear anti-corruption and anti-bribery policies that align with the Bribery Act, the FCPA (Foreign Corrupt Practices Act), and other regional regulatory standards.
- Collaborate with law enforcement when handling high-risk fraud cases and ensure data is readily available and correctly stored.
- Invest in specialized compliance software that tracks sanctions lists, and regulatory changes across multiple jurisdictions.
- Set up internal compliance audits at regular intervals to assess alignment with government policies and international standards.

DISCOVER HOW TO SPOT LEGITIMATE BUSINESSES →

Economic Health

Be prepared for fraud stemming from economic instability by implementing financial resilience and proactive monitoring.

- Closely monitor economic indicators such as GDP growth, inflation, unemployment rates, and cost of living to anticipate increased fraud risk during periods of economic stress.
- Provide financial literacy training for employees to improve awareness of common fraud tactics and how they relate to current economic pressures.
- Perform enhanced due diligence when working with partners in regions experiencing economic instability.
- Incorporate stress testing into your risk management framework, simulating fraud scenarios during economic downturns to ensure preparedness.
- Set up contingency plans that address fraud risks during economic crises, such as increased customer verification processes or tighter transaction monitoring.
- Regularly review third-party risk management strategies to ensure partners remain solvent and compliant during periods of economic instability.

EXPLORE OUR LEARNING COURSES →

What's next?

Now that you've got the steps to boost your fraud defenses, it's time to take action. Our acclaimed annual Identity Fraud Report is coming soon so you can learn the solutions to protect your business.