

IDENTITY VERIFICATION COMPLIANCE CHECKLIST



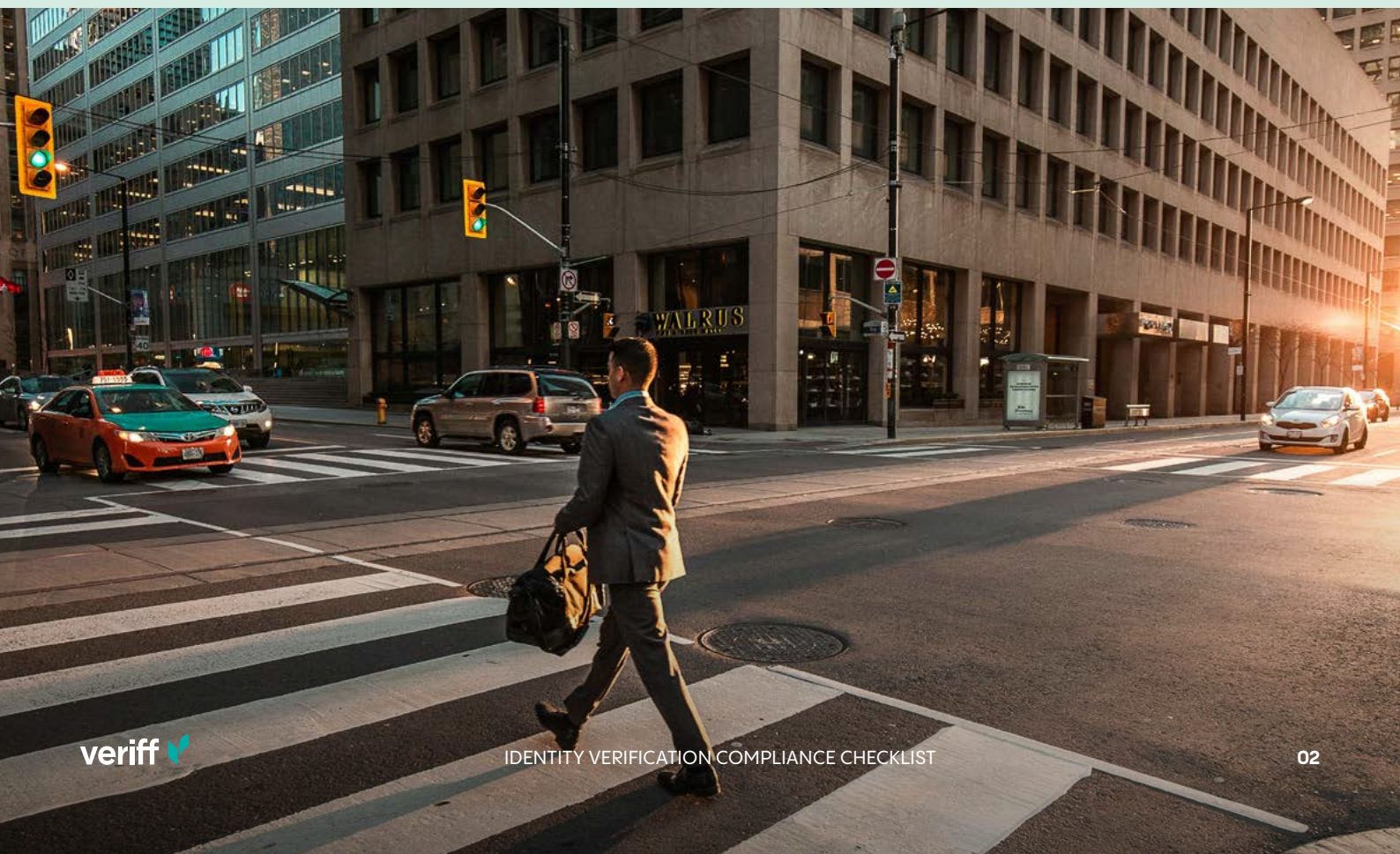
Essential Guide for Financial
Services Startups and SMBs



Introduction

Strengthen your compliance posture with this practical checklist — designed for startups, small and medium-sized (SMBs) and compliance leaders in financial services. The guide outlines key steps to streamline identity verification workflows, minimize fraud risk, and safeguard sensitive customer data with clarity and efficiency. While the checklist reflects common requirements across global Anti-Money Laundering (AML) and data protection frameworks, businesses must ensure that solutions are adapted to meet the specific regulations of their jurisdiction.

Disclaimer: This checklist is provided for informational purposes only and does not constitute legal advice. Please consult qualified legal counsel to confirm compliance with applicable local laws and regulations.



01

UNDERSTAND REGULATORY REQUIREMENTS FOR FINANCIAL SERVICE PROVIDERS

Research local, regional, and global laws: Familiarize yourself with key regulations such as:

- ☐ **Anti-Money Laundering (AML)** laws including customer due diligence requirements formerly known as Know Your Customer (KYC).
- ☐ **Sanctions laws** (e.g., OFAC, UN, EU, and Interpol watchlists).
- ☐ **Privacy laws**, including region-specific regulations such as:
 - General Data Protection Regulation (GDPR) in Europe
 - US State Privacy Laws, such as the California Consumer Privacy Act (CCPA)
 - UK Data Protection Act (DPA)
 - Personal Data Protection Act (PDPA) in Singapore
 - Lei Geral de Proteção de Dados (LGPD) in Brazil
 - Privacy Act 1988 in Australia

Engage a legal advisor: Consult compliance professionals or legal advisors to ensure your organization's practices align with applicable laws and evolving regulatory requirements.

02

GATHER REQUIRED DOCUMENTATION

Collect essential customer documents: Obtain government-issued IDs, proof of address (utility bills, credit card statements, etc.), and tax identification numbers when applicable.

- ☐ **For individuals:** Government-issued IDs, proof of address, tax identification numbers, and biometric data (if applicable). Require a selfie or liveness check to confirm the person presenting the ID is the rightful owner and a real individual, helping prevent identity fraud.
- ☐ **Verify document validity and authenticity:** Check expiration dates, authenticity markers (e.g., watermarks, holograms), and consistency across documents.
- ☐ **Standardize document requirements:** Create a clear checklist for onboarding, specifying acceptable formats (e.g., PDF, JPG) and timeframes (e.g., issued within the last three months).

03 IMPLEMENT VERIFICATION METHODS

- ☐ **Adopt a multi-faceted approach:** Use diverse verification methods to strengthen your process. For example:
 - ☐ Document verification with NFC (Near Field Communication) and optical character recognition (OCR) tools to extract and validate data quickly.
 - ☐ Biometric verification such as facial recognition, with liveness detection to confirm a user's identity.
 - ☐ Database checks that cross-reference customer information with trusted databases like credit bureaus, government databases, and global
- ☐ **Leverage multi-factor authentication (MFA):** Use robust factors like biometrics, authenticator apps, or passkeys to strengthen security beyond passwords or SMS codes.
- ☐ **Integrate risk-based AML measures:** Scale verification to customer risk, requiring stronger methods (e.g., biometrics or passkeys) for high-risk profiles while streamlining low-risk flows.

04 CHOOSE PROVEN SOFTWARE & TECHNOLOGY

- ☐ **Invest in scalable solutions:** Select software that grows with your business, easily adapting to increased customer volumes and new regulatory frameworks.
- ☐ **Prioritize security and compliance features:** Look for tools that offer advanced encryption, fraud detection algorithms, and compliance reporting capabilities.
- ☐ **Evaluate vendor credentials:** Verify your vendor's certifications, such as ISO 27001 for information security management or SOC 2 Type II for data privacy.
- ☐ **Stay ahead with emerging technologies:** Adopt AI-driven tools to automate identity checks, blockchain for secure data storage, or decentralized digital ID solutions.

05 CONDUCT MULTI-LAYERED VERIFICATION

- ☐ **Combine automated and manual processes:** While automated systems provide speed and accuracy, manual reviews offer critical oversight to detect subtle inconsistencies.
- ☐ **Implement dynamic testing:** Randomly test user-provided data against varied sources to identify fraudulent or mismatched information.
- ☐ **Strengthen fraud detection:** Use AI and machine learning to flag abnormal activity such as multiple account creation attempts from the same device or location.

06 ENSURE COMPREHENSIVE DATA PRIVACY MEASURES

- ☐ **Encrypt data end-to-end:** Encrypt sensitive customer data both in transit and at rest using strong encryption protocols like AES-256.
- ☐ **Data minimization principle:** Only collect and store customer data that is necessary for your operations. Reduce risks by deleting outdated records.
- ☐ **Comply with data protection laws**
- ☐ **Archive consent records:** Maintain an audit trail that shows users agreed to data collection and understand how you will use their information.
- ☐ **Routine audits and employee training:** Regularly review your data policies, conduct privacy impact assessments, and educate employees about handling sensitive information.

07 ONGOING MONITORING AND RISK ASSESSMENT

- ☐ **Real-time monitoring:** Continuously monitor for suspicious activities such as unusual IP addresses, high-value transactions, or multiple failed login attempts.
- ☐ **Periodic customer re-verification:** For higher-risk customers, schedule re-verification cycles. For example, update KYC information annually for active accounts.
- ☐ **Use alerts and reporting tools:** Set up alerts for activities such as mismatches in beneficiary details or transactions to high-risk jurisdictions. Regularly generate reports for compliance audits.
- ☐ **Scale with industry needs:** Adjust monitoring methods to match transactional volumes. For example, businesses handling cryptocurrency may require tools to trace digital wallet origins.

08 TRAIN YOUR TEAM

- ☐ **Comprehensive onboarding:** Provide new hires with training programs on compliance basics, identity verification procedures, and best practices.
- ☐ **Ongoing learning:** Host regular workshops or webinars to update employees on new threats, regulations, and tools.
- ☐ **Incident management protocols:** Train employees on how to respond to potential breaches, suspicious activity, or fraudulent attempts swiftly and effectively.
- ☐ **Empower key roles:** Assign compliance champions who can act as go-to resources for team members with questions or concerns.

09 CONSIDER INDUSTRY-SPECIFIC NEEDS

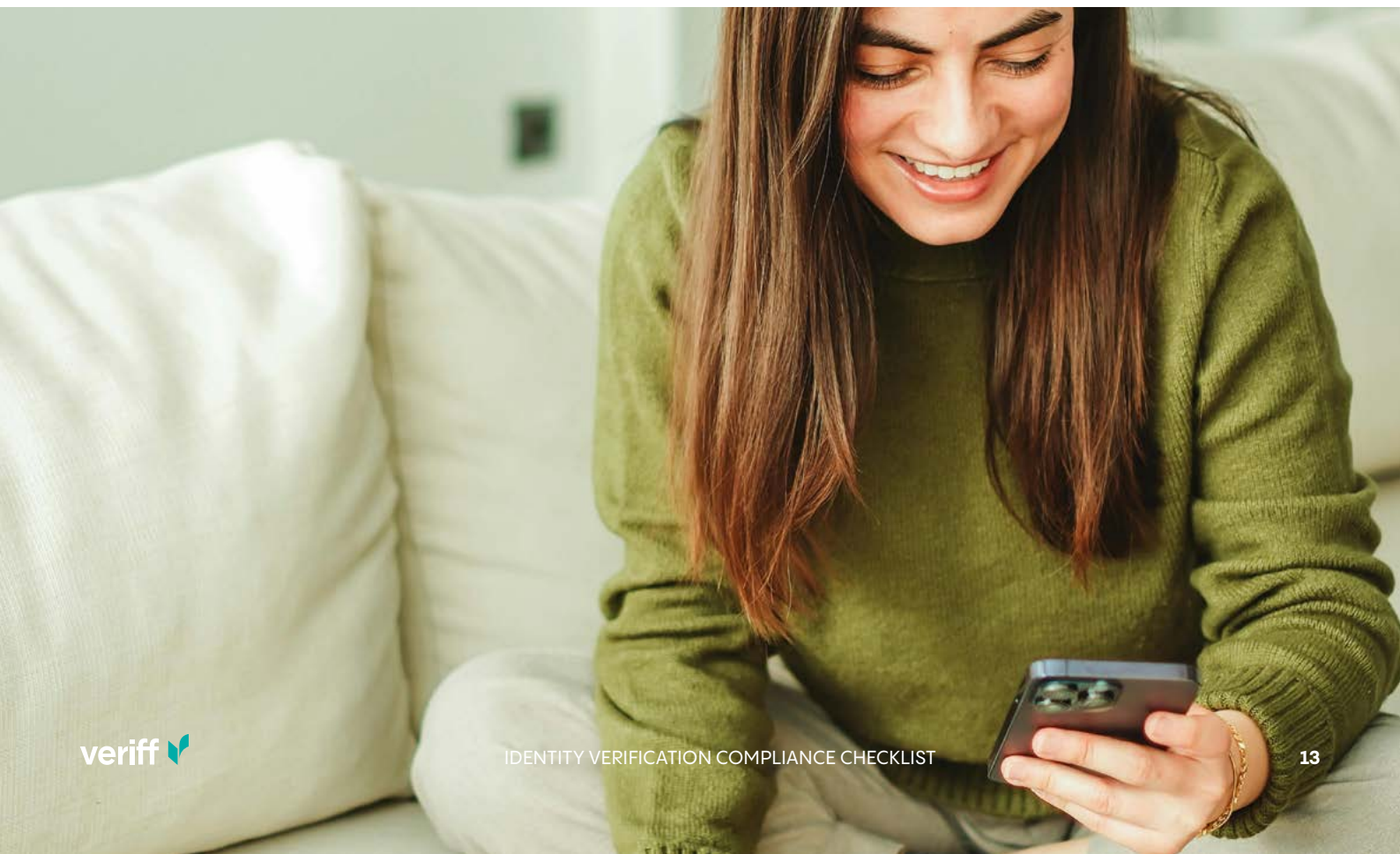
- ☐ **Fintech and banking:** Integrate with electronic KYC (eKYC) platforms and fintech-friendly APIs.
- ☐ **Retail and eCommerce:** Focus on payment fraud detection and maintain active PCI DSS compliance.

10 REVIEW AND OPTIMIZE REGULARLY

- ☐ **Audit your systems periodically:** Schedule compliance audits to ensure all processes align with both your industry's best practices and regulatory changes.
- ☐ **Gather feedback:** Ask customers about their onboarding experience and identify pain points in your verification process.
- ☐ **Invest in continuous improvement:** Use auditing and customer feedback results to upgrade your tools, processes, and workflows. Stay agile as your business scales.

HOW VERIFF CAN HELP PREVENT IDENTITY FRAUD AND STAY COMPLIANT

Startups and SMBs can leverage Veriff, a powerful identity verification platform, to strengthen their compliance framework and reduce the risk of fraud. Veriff's key features directly align with the priorities outlined in this checklist, offering reliable and scalable solutions for modern businesses.





Veriff is a global identity platform helping businesses build trust online. Our AI-native technology combines automation and human expertise to quickly and accurately verify users worldwide with minimal friction.

Our trust infrastructure helps businesses stay compliant, prevent fraud, protect users, and scale globally, enabling a safer, more transparent internet for everyone.

Speak to one of our fraud experts today to discover how we can create customizable fraud protection for your business:

veriff.com