

SII Risk Mitigation Resource

Regulatory & AML Compliance Risk

- **The Risk:** Accepting alternative or non-documentary identity verification might trigger internal or external Anti-Money Laundering (AML) audit failures.
- **Mitigation Strategy:** Shift the burden of verification to a structured multi-agency model. By executing a formal MOU with a vetted Survivor Support Organization (SSO), the bank treats the SSO's official attestation letter as a secondary verified record rather than bypassing Know Your Customer (KYC) entirely.

Operational & Retraumatization Risk

- **The Risk:** Front-line bank workers (tellers, branch staff) may inadvertently interrogate a survivor regarding missing documents, triggering intense re-traumatization or forcing the client to leave.
- **Mitigation Strategy:** Implement the "**Warm Hand-Off Protocol**." Front-line retail workers are strictly barred from processing or auditing SII accounts. When an applicant presents an alternative intake packet, the teller routes the transaction directly to an isolated, pre-trained Tier-2 compliance team.

Digital Surveillance & Security Risk

- **The Risk:** Traffickers or abusers frequently use digital tracking, spyware, or compromised email accounts to track a survivor's assets, potentially breaching the bank's digital perimeter or discovering the survivor's location.
- **Mitigation Strategy:** During account onboarding, multi-factor authentication (MFA) must be tied strictly to a newly issued, secure device verified by the SSO. Additionally, the bank must isolate client profiles within internal databases so that generic CRM notes never contain references to keywords like "trafficking" or "shelter".

Credit & Fraud Flag Overrides (Coerced Debt)

- **The Risk:** Automated automated screening systems (ChexSystems or LexisNexis) will automatically block applicants due to historic unpaid debts or fraudulent accounts opened by their abusers.
- **Mitigation Strategy:** Create an institutional exception pipeline. Under the [Debt Bondage Repair Act \(DBRA\)](#) in the United States and global equivalents, the compliance liaison overrides these flags if they match the documentation provided in the SSO intake form.