Combating Financial Crime: Agentforce Opportunities in Singapore's Banking Sector

Whitepaper

Table of Contents

01 Executive Summary

Financial crime in Singapore is escalating in scale and sophistication, fuelled by rapid digitalization, AI-enabled criminal tactics, crypto adoption, and cross-border enforcement complexity. As reported by the Straits Times, since 2019 victims in Singapore have lost more than S$3.4 billion to scams, including a record S$1.1 billion in 2024; 2025 year-to-date losses exceed S$535 million with over 22,200 cases reported, underscoring the urgency for banks and digital businesses to modernize their defences. Business leaders are acutely aware: 76% of Singapore executives are concerned about financial crime in 2025, above the global average (~70–71%) and 82% of APAC senior management expect risks to rise further this year.

Since 2019, scams in Singapore has amount to more than S$3.4B

Root causes concentrate around four drivers. First, Singapore's advanced economy and pervasive online ecosystems (remote banking, e-commerce, social media) have expanded attack surfaces. In fact, ~60% of scams originate on messaging apps and social platforms, where fake ads and influencer endorsements entice victims. Second, despite its immense business benefits to organisations, criminals can also use AI as a tech advantage. 61% of executives cite AI-enabled crime (deepfakes, synthetic identities, voice cloning) as a key enabler, and crypto-related risks are a significant concern for 74% of executives while only 36% report adequate safeguards. Third, social engineering and rising cost of living standards drives many self-effected transfers, with scammers exploiting trust, fear and urgency cues. Fourth, Singapore's role as a global financial hub brings both opportunities and challenges, including exposure to financial crime risks. The rise of cross-border crypto and digital fraud adds complexity to coordinated enforcement efforts.

The strategic implication for banks is that rule-based legacy controls and siloed tools cannot match the speed and coordination of modern financial crime. Institutions need interoperable, AI-driven orchestration that connects detection, intelligence, KYC/CLM, case management, and customer communications in near-real time with governance and auditability by design.

Agentforce addresses this need with secure, compliant, AI agents that automate and coordinate fraud prevention and investigations end-to-end. It combines (1) proactive detection and response with real-time anomaly spotting, automated alert triage, and investigator-ready case briefs; (2) provides AI governance through its Einstein Trust Layer, encryption, and fine-grained access controls (including Anti-Bribery and Anti-Corruption) for safe, auditable operations; and (3) ensures customer protection at scale with 24/7 agents across channels to educate, verify, and de-risk interactions. Crucially, Agentforce is interoperable via Mulesoft Agent Fabric to orchestrate third-party FinCrime tools such as Quantexa and Fenergo, as well as support agent-to-agent (A2A) operating models, extending the scope of agentic solutions from a single platform to an enterprise-wide, best-of-breed ecosystem.

With an interoperable, governed, A2A architecture, this places Singapore banks in positions to reduce losses, increase regulatory confidence, and protect customers while scaling FinCrime operations without linear headcount growth.

Agentforce addresses the need to combat modern financial crime with secure, compliant, AI agents that automate and coordinate fraud prevention and investigations end-to-end.

02

Financial Crime in Singapore: Current Landscape and Implications

2.1 Current State Overview

Financial crime in Singapore has escalated to unprecedented levels, driven by digital transformation, advanced criminal tactics, and economic uncertainty. Since 2019, Singapore has lost over $3.4 billion to scams, with a record $1.1 billion in 2024. In 2025 alone (up to August), there have been 22,200 scam cases, resulting in $535.2 million in losses. Investment scams remain a major contributor, accounting for more than $23 million in July 2025[1]. Some of the key trends include:

AI-Driven Crime

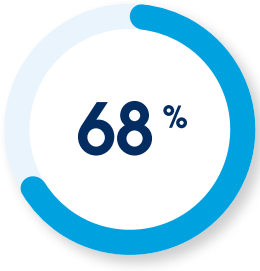
Criminals are leveraging artificial intelligence to create synthetic identities, deepfakes, and automated fraud campaigns.

Cybersecurity Risks

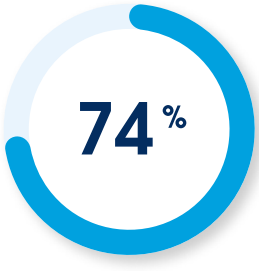
68% of executives cite cybersecurity as their top concern, while 61% highlight AI-enabled fraud as a growing threat[2].

Crypto Vulnerabilities

74% of executives view cryptocurrency-related crime as a significant risk, yet only 36% have safeguards in place[2].



of execs cite cyber security as top concern



of execs view crypto crime as significant risk

[1]The Straits Times. Scam tracker: What are the latest trends in S'pore, and how much money has been been lost.

[2]The Straits Times. Three-quarters of senior executives in Singapore flag worries about financial crime risks in 2025.

Money Laundering

Singapore's role as a global financial hub makes it a prime target.

Exploitation of digital advertising and social media

Fake ads and influencer endorsements lure victims into fraudulent schemes; additionally, social platforms are increasingly used for phishing and investment scams, eroding consumer trust and brand integrity.

Unsurprisingly, 76% of Singapore executives are concerned about financial crime in 2025, exceeding the global average of 71%. In Asia-Pacific, 82% of senior leaders expect financial crime to rise, the highest globally[2].

[2]The Straits Times. Three-quarters of senior executives in Singapore flag worries about financial crime risks in 2025.

2.2 Identified Root Causes

The convergence of digitalization, advanced criminal tactics, human vulnerabilities, regulatory challenges, and economic pressures has created a perfect storm for financial crime in Singapore. This includes:

Digitalization & Online Ecosystems

Singapore's advanced digital economy and high GDP per capita make it an attractive target for scammers. 60% of scams occur through messaging apps and social media, where fake ads and influencer endorsements lure victims into fraudulent schemes[3]. The rapid adoption of remote banking, e-commerce, and social media marketing has opened new avenues for fraud.

Sophisticated Technology Use by Criminals

Criminals are leveraging advanced technologies to scale and automate fraud. Theses AI-driven tactics – such as deepfakes, synthetic identities, and fake voices – act as major enablers of financial crime.

Human Factors and Economic Pressures

Scammers exploit universal human emotions like greed, fear, and trust. Rising cost of living and economic uncertainty have fuelled financial insecurity, making individuals more susceptible to scams promising quick returns. Thus, many scams involve self-effected transfers, where victims willingly transfer money after being manipulated.

Regulatory & Enforcement Gaps

Singapore's role as a global financial hub makes it a "North Star" for criminals, particularly for money laundering. Furthermore, the cross-border nature of crypto and digital fraud complicates enforcement, as criminals exploit regulatory differences across jurisdictions.

The convergence of digitalization, advanced criminal tactics, human vulnerabilities, regulatory challenges, and economic pressures has created a perfect storm for financial crime in Singapore. Addressing these root causes requires multi-layered strategies, including AI-driven fraud detection, stronger compliance frameworks, and consumer education.

[3]www.mha.gov.sg/home-team-news/story/detail/mha-cos-2025--working-together-to-fight-scams/

03 Introduction to Agentforce and MuleSoft Agent Fabric

3.1 What is Agentforce?

Agentforce is Salesforce's AI-powered agent platform designed to deliver secure, compliant, and intelligent automation across customer and operational workflows. Agentforce emerges as a timely solution designed to assist Singapore banks in three critical areas:

Proactive Fraud Detection & Response

- **Real-time anomaly detection** for fraud prevention and risk scoring, and surveillance of transactions and behaviours before they escalate
- **Scalable and configurable workflows** to handle high volumes of tasks without increasing headcount, and automates large volumes of repetitive compliance tasks like alert triage, case management, and KYC/AML checks

AI Governance & Compliance Built-In

- **Einstein Trust Layer** ensures data security, prevents prompt injection, and maintains full audit trails for regulatory compliance
- **Attribute-based access control (ABAC) and encryption** protect sensitive financial data across all interactions

Customer Protection & Education at Scale

- Provide customers with **24/7 availability** by deploying Agentforce agents across digital channels (chat, email, social) to educate customers on scam prevention and guide them through secure processes
- **Sentiment analysis** to detect distress signals and escalate high-risk cases to human investigators immediately

3.2 Interoperability of Agentforce with MuleSoft Agentic Capabilities

Financial crime isn't a single-step event; it's a chain of behaviors that spans onboarding, payments, trade, communications, and identity. Stopping it requires multiple, specialized capabilities acting in concert, more specifically, the orchestration across banking architectures to unify applications, data sources, and workflows. While Agentforce is designed with executing specific use cases at its core, MuleSoft Agent Fabric is Salesforce's enterprise-grade solution for agentic governance and orchestration, purpose-built to address the challenges of scaling AI-driven fraud detection in regulated environments. Here are 3 key differentiators where this architecture approach is more robust and suitable for banks:

Orchestration Through Integration Platforms

For Agentforce to work seamlessly with leading FinCrime platforms (Quantexa, Fenergo, Actimize) and other AI agents, MuleSoft Agent Fabric acts as the "central nervous system" to orchestrate across these diverse agents, enabling coordinated fraud detection, investigation, and reporting, shrinking time-to-detect and improving decision quality. For example, a fraud detection agent can trigger an entity resolution agent to enrich alerts, while a KYC agent retrieves due diligence information–all within a unified workflow. This integration eliminates silos, accelerates response times, and ensures that fraud investigations and compliance processes are consistent across the enterprise.

Enterprise AI governance via a Unified Platform

MuleSoft Agent Fabric enforces strong governance across all AI agents in the FinCrime ecosystem. This means every agent interaction, whether it's fraud detection, KYC checks, or case management, is subject to enterprise-grade security, privacy, and compliance controls. Sensitive data is protected through encryption and access controls, and all agent actions are automatically checked against regulatory requirements (such as MAS and FATF standards). This governance layer helps banks confidently deploy AI at scale, knowing that every autonomous decision is safe, compliant, and auditable.

Visualisation and Audit Trail

Regulatory transparency is critical in financial services. MuleSoft Agent Fabric's Agent Visualizer automatically records every agent-to-agent interaction and decision, creating a comprehensive, auditable trail. This means banks can easily demonstrate to regulators how decisions were made, which agents were involved, and what data was accessed. These audit trails not only support compliance and internal investigations but also build trust with customers and stakeholders by showing that AI-driven processes are transparent and accountable.

3.3 Practical Use Cases with Agentforce

Agentforce can be rapidly deployed to address critical financial crime challenges, delivering measurable business impact. Below are three high-value use cases:

Know-Your-Customer (KYC) / Customer Due Diligence (CDD) Automation

Agentforce streamlines traditionally manual and time-consuming KYC/CDD processes by leveraging Retrieval-Augmented Generation (RAG) to automate ingestion and validation of client documents (ID, proof of address, financial statements), detects expiration, ensures completeness, and applies onboarding checklists. Business benefits include:

- Reduces onboarding time and friction
- Improves accuracy and consistency across jurisdictions
- Enhances operational efficiency for middle-office managed service environments

Risk Scoring Automation

Agentforce enhances client risk profiling by aggregating and analyzing internal and external data sources using configurable rules and AI-driven insights. It can dynamically adjust due diligence levels based on evolving risk indicators (transaction patterns, geography, adverse media) and triggers escalations when thresholds are breached. Business benefits include:

- Enables predictive, real-time risk assessment
- Reduces manual effort and false positives
- Optimizes resource allocation for compliance teams

Regulatory Compliance Management

Agentforce automates the preparation, validation, and submission of mandatory regulatory filings. It can extract key data points, validate against regulatory requirements, and generate submission-ready documentation with full audit trails. Business benefits include:

- Cuts manual data analysis by up to 30%
- Reduces risk of errors and missed deadlines
- Strengthens confidence in meeting Monetary Authority of Singapore, Financial Action Task Force, and global compliance standards

reduction in manual data analysis with Agentforce

04 Final Thoughts and Next Steps

The data paints a clear picture: rising losses (S$1.1 billion in 2024; S$535 million+ YTD 2025), social-platform-driven scams (~60%), and executive concerns above global averages demand faster, coordinated defences that go beyond point solutions. Agentforce's A2A + interoperability pattern is purpose-built for this moment.

To move from awareness to action, financial institutions should prioritize three immediate steps:

Assess Current Gaps and Integration Readiness

Conduct a rapid diagnostic of your FinCrime ecosystem across transaction monitoring, KYC/CLM, case management, and customer engagement to identify silos and manual choke points. Evaluate whether your integration layer can support real-time orchestration across these systems.

Pilot AI-Driven Orchestration with Agentforce

Start with a controlled proof of concept focused on a high-impact use case, such as real-time payment fraud or mule account detection. Leverage Agentforce's ability to integrate with existing tools like Quantexa and Fenergo, and demonstrate the value of agent-to-agent (A2A) collaboration and orchestrator agents in reducing time-to-detect and improving decision quality.

Establish Governance and Human-in-the-Loop Controls

Define escalation thresholds, audit requirements, and ethical guardrails to ensure compliance and trust. Use the Einstein Trust Layer and ABAC to enforce data security and regulatory alignment from day one.

For the Singapore banks that embrace the interoperable, agent-to-agent ecosystem now won't just lead the market; they'll redefine it, setting the tempo of innovation, anticipating risk before it emerges, and establish brand trust and value to customers at a global scale.

05 Salesforce and PwC Partnerships

PwC + Salesforce: Powering the Next Era of AI-Driven Business.
PwC and Salesforce empower organizations to confidently navigate complexity, unlock AI-driven innovation, and build trust at every step of their AI journey with a human-led, tech-driven approach. With our deep industry experience, we have award-winning solutions and capabilities to help you enable the overall potential of your Salesforce Customer 360, while putting trust at the heart of your Salesforce transformation. Learn how to enhance your Salesforce investment and unite your sales, service, marketing, commerce, IT, and analytics around the most valuable asset of your business – your customers.

For more details, please visit https://www.salesforce.com/partners/pwc/