Deloitte.

Insights into current payment fraud trends and future developments

Madan Sathe & Konrad Schwenke

04 November 2025

Introduction Payment Fraud

Fraud is a critical and growing challenge for the financial services sector which can be demonstrated by quantitative and qualitative factors

Recent News

Statistics

Total value of reported **payment fraud** in the EEA for 2022[1]

€4.3bn

Increase of Cyberfraud in Switzerland between 2020 and 2024[2]

159%

Percentage of adults globally who **lost money** to scammers in the last 12 months[3]

23%

Survey respondents who believe **banks should always be responsible** for reimbursing scam victims[3]

45%

Sources: [1]Report on payment fraud, EBA & ECB, 2024; [2]Swiss Cybercrime statistics, Federal Statistics Agency, 2025; [3]Global State of Scams, Global Anti-Scam Alliance, 2025

Examples of payment fraud across the customer journey

Payment fraud can be classified into unauthorized and authorized party fraud with further differentiation by perpetrator, channels and methods

Unauthorized Party Fraud

Identity Fraud

Fraudster obtains the personal and/or financial information of another person to use their identity to commit fraud

Man-in-the-Middle Fraud

Fraudster intercepts the communication and/or alters the transaction instructions

Compromised Credentials Fraud

Fraudster gets access to victim's MFA device (e.g., mobile phone and/or SIM for OTPs) which is then used to authenticate the transactions

Phishing Fraud

Fraudster directs the victim to a website replicating bank's payment page to steal victim's banking credentials

Authorized Party Fraud

Impersonation Fraud

Fraudster impersonates a legitimate entity (e.g., a friend, a supplier) to trick the victim into sending the funds to an account controlled by the fraudster

Business Email Compromise Fraud

Fraudster sends an email that appears to come from a known source (e.g., supplier) to trick the victim

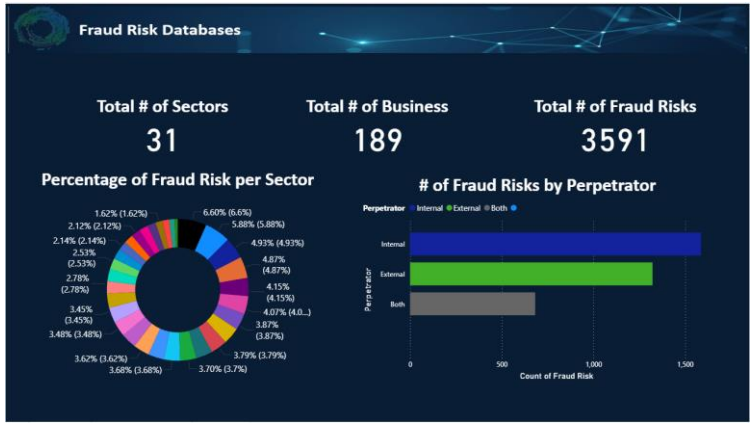
Relationship Fraud

Fraudster pretends to be interested in the victim in order to manipulate and gain control of the victim's account information

Money Mule Fraud

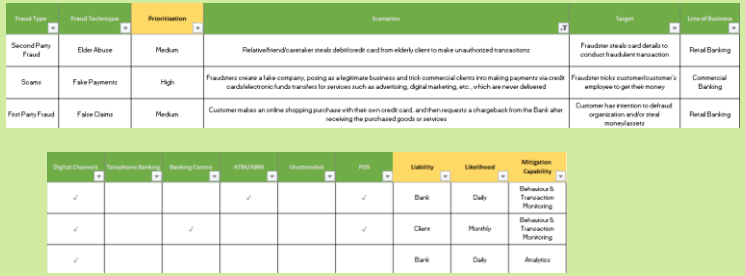
Fraudster convinces the victim to receive fraudulent payments in victim's account, which are then redirected to the fraudster

Deloitte. Fraud Risk Database



Banking & Payments specific fraud risks

- For the Banking & Payments sector our database contains 184 specific fraud risks with an emphasis on external perpetrators
- It allows to filter by fraud type, typical targets and liability holders



Note: *Unauthorized Party Fraud* is when an unauthorized party creates / takes over an account or misuses account information / payment instrument
Authorized Party Fraud is when an authorized party is manipulated by misrepresentation or misdirection

Fraud trends and challenges for Swiss banks

We are seeing unprecedented change in the fraud landscape and Switzerland is an attractive target for fraudsters due to the relatively high wealth of Swiss banking customers

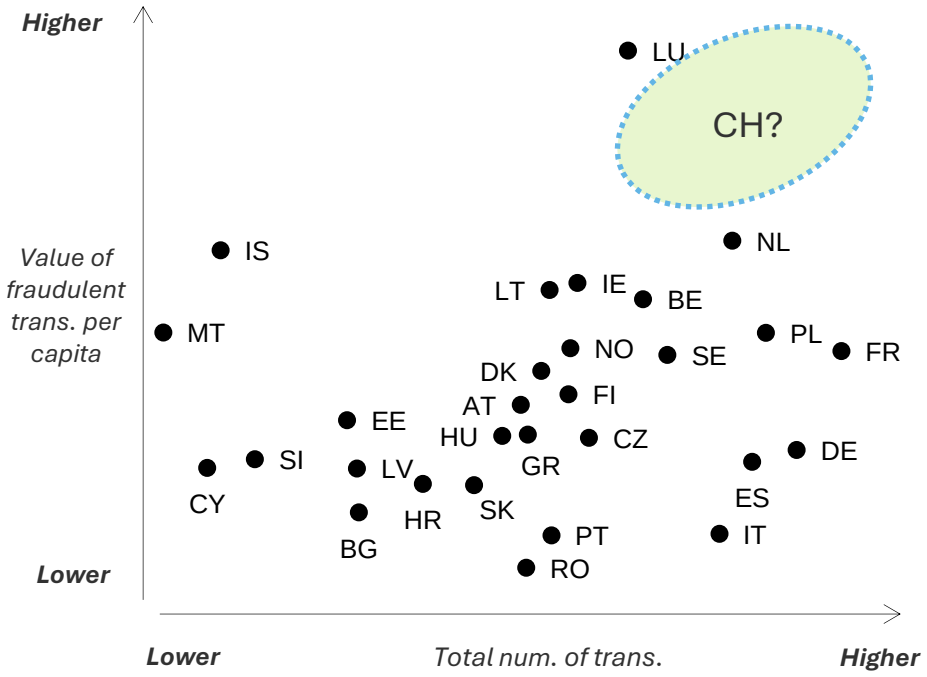
Increasing **sophistication** of fraudulent actors and involvement of **organised crime**

Dispersed **ownership** for fraud risk management and lack of ecosystem/data sharing models

Perpetrators, including **money mules**, among the **client population** are not identified

Technology enables new fraud methods (e.g. **Deep Fakes**) and changes in the payment landscape (e.g. **P2P, Instant Payments**, **Agentic Payments**)

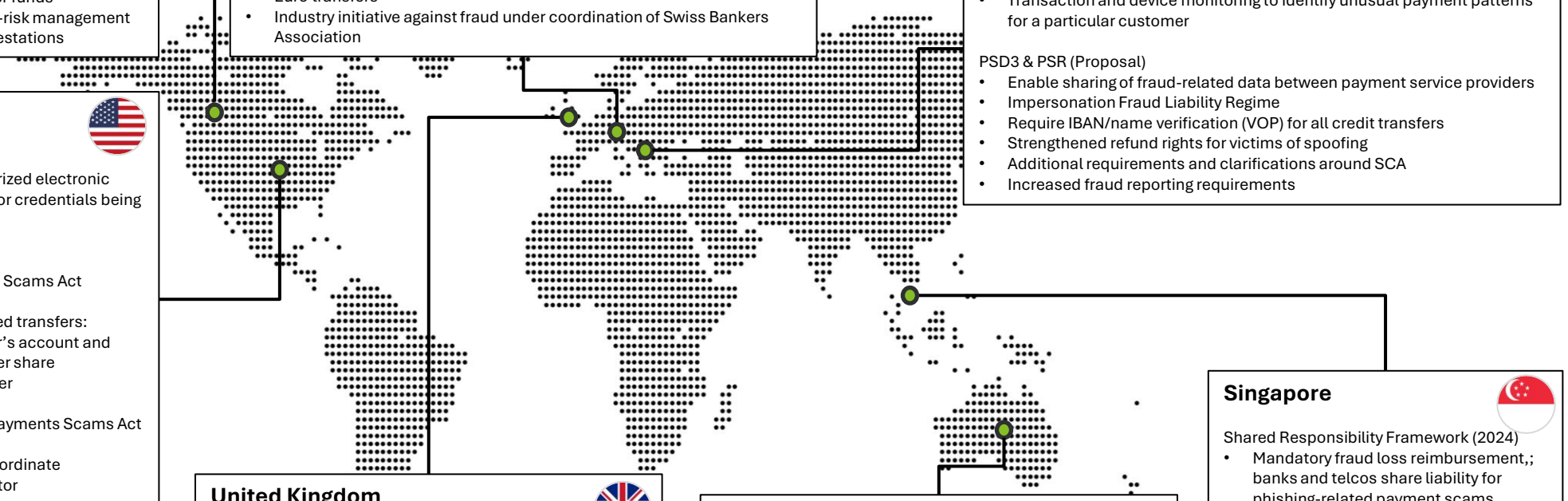
Regulatory changes expanding bank liability for fraud due to increased media attention & public pressure



Source: Report on payment fraud, EBA & ECB, 2024 – data for H1 2023

Fraud Regulation Overview

Recent years saw an increase in fraud regulation worldwide also affecting expectations of customers and business partners of Swiss banks



Canada

Retail Payment Activities Act & Regulation (2024, 2025)
- Obligations for incident detection, reporting, fraud-risk controls, and safeguarding of end-user funds
- Mandatory operational-risk and fraud-risk management programs and annual compliance attestations

Switzerland

- Currently no dedicated payment-fraud regulation
- EU spillover: Swiss PSPs participating in SEPA must support EU VOP for Euro transfers
- Industry initiative against fraud under coordination of Swiss Bankers Association

EU

PSD2 (2015):
- Requires strong customer authentication (SCA) for electronic payments
- Transaction and device monitoring to identify unusual payment patterns for a particular customer

PSD3 & PSR (Proposal)
- Enable sharing of fraud-related data between payment service providers
- Impersonation Fraud Liability Regime
- Require IBAN/name verification (VOP) for all credit transfers
- Strengthened refund rights for victims of spoofing
- Additional requirements and clarifications around SCA
- Increased fraud reporting requirements

United States of America

Electronic Fund Transfer Act (1978, 2021)
- Requires reimbursement for unauthorized electronic transfers, including access to device or credentials being obtained fraudulently by a third-party
- Does not cover APP style scams

U.S. Protecting Consumers from Payment Scams Act (Proposal introduced 2024)
- Shared liability for fraudulently induced transfers: financial institution holding consumer's account and institution receiving fraudulent transfer share responsibility for reimbursing customer

Task Force for Recognizing and Averting Payments Scams Act (Proposal introduced 2025)
- Creation of a national task force to coordinate government agencies and private sector

Global

ISO 20022 messaging
- Better tracking and tracing of payments due to more structured data accompanying payments
- Improving interoperability between banks
- In Switzerland applied since 2020

World Bank / BIS Fast Payments Toolkit (since 2021)
- Fast payments system toolkit to support countries in implementing fraud resilient instant payment systems

United Kingdom

UK Anti-fraud Act (2024)
- Failure to prevent fraud offence with an unlimited fine
- Reasonable procedures to prevent fraud required

UK Payment (Amendment) Regulation (2024)
- Fraud Prevention: Permission for banks to delay faster payments if there is suspicion of fraudulent behaviour (authorised push payment fraud)

PSR Reimbursement Regime (2024)
- Fraud Protection: Mandatory Reimbursement for APP fraud victims

Australia

Scams Prevention Framework (2025)
- Whole-of-ecosystem approach: banks, telecommunication providers, digital platform services providers
- Regulators empowered; Civil penalties for non-compliance; Reporting obligations to regulators and other businesses
- Mandatory information sharing coordinated by National Anti-Scam Centre
- Mandates user-friendly methods for consumers to notify banks and block transfers ("kill switch")

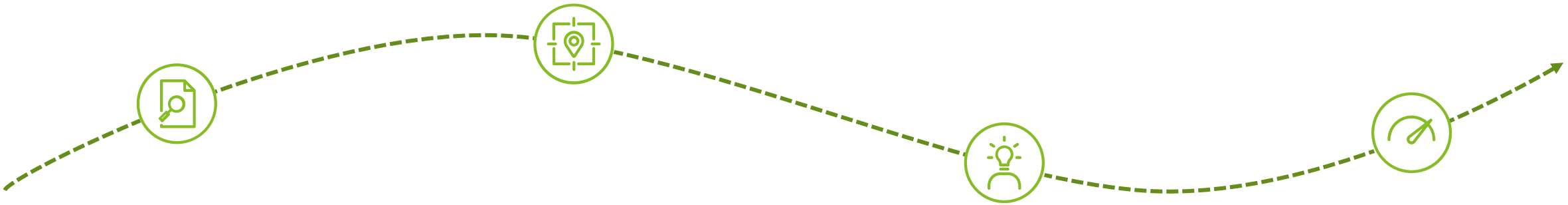
Singapore

Shared Responsibility Framework (2024)
- Mandatory fraud loss reimbursement,; banks and telcos share liability for phishing-related payment scams
- Focus is on phishing and impersonation scams
- Requires real-time alerts, 12-hour cooling-off periods, and "kill switch" mechanisms for customers to block transfers
- Financial institutions are first in line having to reimburse the customer if they did not fulfil their obligations

Protection from Scams Bill (2025)
- Police empowered to issue restriction orders to block scam-linked transfers

Fraud risk management programme

Developing a strong fraud risk management program starts with a detailed horizon fraud risk and current state assessment from which potential changed to the fraud risk operating model follow



Vision and Fraud Risk Assessment

Design Target Operating Model

Implement changes

Monitor and Optimize

Design Target Operating Model for Fraud Risk Management

Deloitte has developed a comprehensive fraud risk framework in line with leading industry practices

Governance	Organization	Prevention	Detection	Response	Post-Fraud actions
Fraud Strategy	Organizational structure for fraud area	Fraud risk management	Transactional monitoring tools	Fraud attack management	Managing recoveries, chargebacks, and refunds
Corporate Fraud Management Policies and Procedures	Fraud roles and responsibilities	Proactive Modus Operandi Analysis	Biometric and device analysis tool	Alert Investigation	Monitoring and improvement of post-fraud actions
Regulation and Competent Authorities	Human resources management	Employee training and awareness	Rule Management	Case Manager	Evidence management
Fraud Technology and Vendor Management	Cross-departmental fraud coordination	Customer and third-party awareness	Tracking and continuous improving of fraud detection	Claims, customer service, and analysis of their automation level	Fraud Recoveries, Chargebacks, and Refunds Standards
Fraud Communication and Reporting Management		Customer authentication and transaction authorization	Artificial Intelligence Predictive Models	Tracking and continuous improving fraud response	
Quality Assurance		Customer onboarding	Bespoke Analytics	Fraud Response Standards	
Fraud Intelligence Sharing		Fraud Prevention by design	Fraud Detection Standards		
		Fraud Prevention Standards			

Deep-Dive: Money Mules

Money Mules are a growing concern with regulatory attention as they are a critical link in the fraud chain, often still located in Switzerland and detecting them within the client population of Swiss banks is an opportunity to make the country less attractive for fraudsters

What are Money Mules?

DEFINITION

Individuals who serve as intermediaries for criminals by transferring illegally acquired money.

ONBOARDING

Knowingly provide services and take a commission for funds laundered or recruited unknowingly via deceptive job offers.

Accounts might be opened with legitimate KYC or using forgeries.

Challenges for Banks

RISK

Money Mules facilitate money laundering, including for fraud, and should as such be reported to the FIU (MROS).

Undetected activity can lead to reputational damage and business restrictions.

DETECTION

Standard AML Transaction Monitoring rules often not fit for purpose to detect money mules.

Problem exacerbated by new payment rails.

Detection Methods

See next slide

Deep-Dive: Money Mule Detection

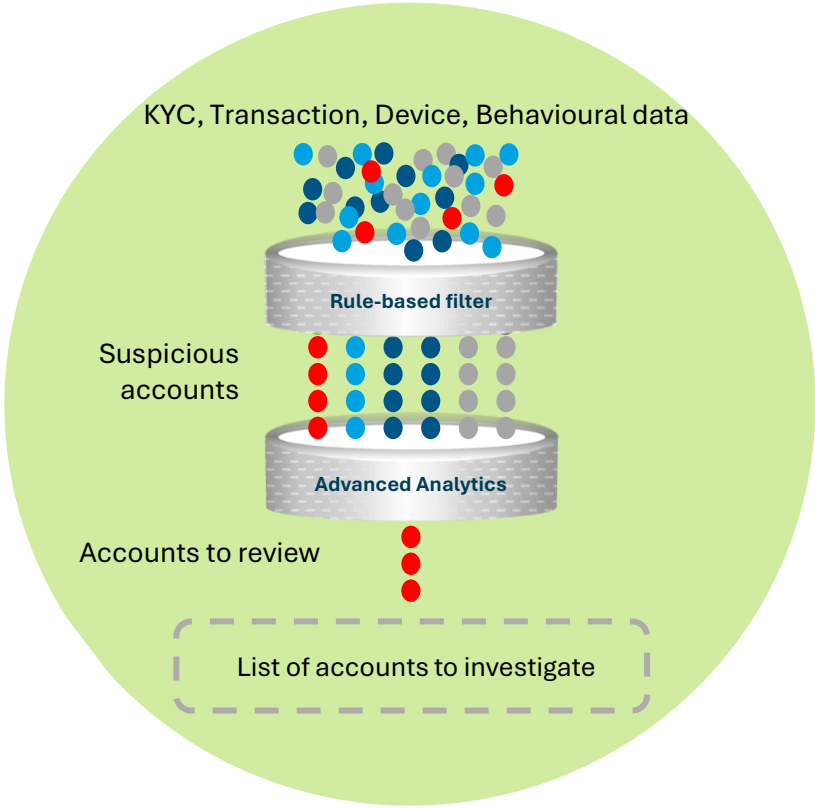
Detecting Money Mules requires a bespoke approach as they often slip through standard Transaction Monitoring

HKMA's Macro Analytics Programme

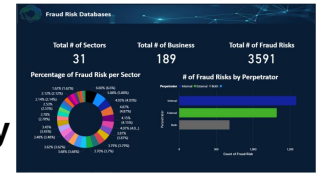
- Deloitte supported the Hong Kong Monetary Authority (HKMA) in setting up a data sharing utility.
- Proof of value focused on pooling data from multiple institutions to detect Money Mule Activity.
- Deloitte facilitated onboarding of banks, agreement on data schema, data validation and analysis.
- The programme yielded an ability to compare the response of banks' to specific threats and identify best practices.
- HKMA could demonstrate how information sharing supports better threat detection and enabled HKMA to plan further development of Macro Analytics to expedite interdiction of mule accounts.

Source: The Digitalisation of AML / CFT Supervision: Where Now and What Next?, 2024

Detection Workflow



Selected indicators from Deloitte's fraud risk library



General:

- Accounts with minimal or no "signs of life"
- Unusual device or IP
- "Jail-broken" or "rooted" devices
- Multiple accounts sharing contact details
- Rapid transfer of funds, also < CHF 10'000
- Unusual currencies/jurisdictions

Re-infiltrated perpetrators:

- Previously closed accounts which were only active for months can serve as a reference:
  - Device fingerprints, IP addresses, and behavioural traits
  - Connection patterns & timings, same IP addresses, countries, same transactional patterns/fingerprints

Detecting deepfakes and synthetic content produced by GenAI

As fraudsters increasingly exploit AI-generated media to manipulate payment processes, advanced detection technologies are essential. Combing AI-powered tools with employee awareness, allows organisations to strengthen security and protect their reputation

Approach for deepfake detection and Technology:

- **AI-Powered Detection:** Utilises deep neural networks to identify in real-time subtle inconsistencies in video and audio deepfakes
- **Multimodal Analysis:** Combines visual and audio signals for more accurate fraud detection
- **Real-Time Screening:** Integrates seamlessly with payment verification systems to flag suspicious transactions instantly

Model Training & Data Sources:

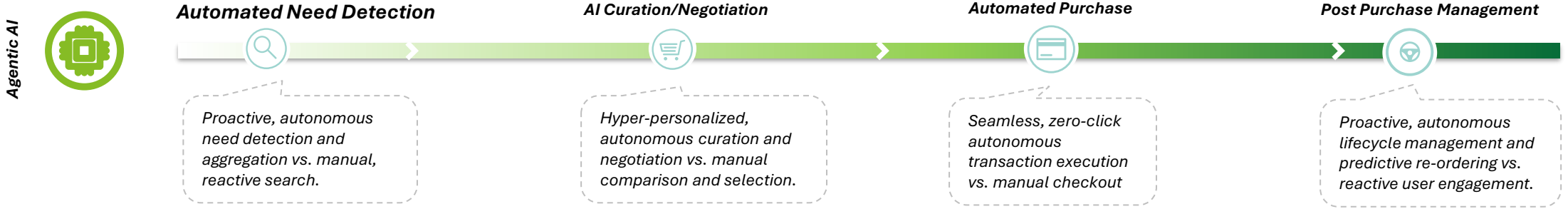
- **Diverse Datasets:** Models are trained on extensive collections of authentic and synthetic media to improve detection accuracy
- **Continuous Learning:** Algorithms are regularly updated with new fraud patterns and emerging deepfake techniques
- **Company-Specific Data:** Incorporates internal fraud cases and external threat intelligence to tailor detection to organisational risks

Employee Awareness:

- **Regular Training:** Employees receive ongoing education on recognising deepfake fraud attempts and using detection tools effectively
- **Verification Protocols:** Staff are encouraged to verify suspicious interactions using AI tools before approving transactions
- **Reporting Mechanisms:** Tools and procedures are in place for employees to escalate suspected deepfake incidents promptly

Future Outlook: AI agents initiating payments

Agentic Payments will advance transaction automation and create new challenges for fraud prevention & detection



Implications for Fraud Risk

- Payments increasingly initiated by AI agents, not humans, will require updates to consent and authorization models
- Fraud detection needs to be redesigned, behaviour-based fraud detection models will not be effective when agents are initiating payments
- Weaknesses in agent authentication protocols or prompt injection could be exploited for unauthorized access
- If an agent is hijacked or its credentials are stolen, it could initiate fraudulent payments at scale and speed

Our Deloitte Fraud Centre of Excellence (CoE) and global experience

Our global network of experts will utilise internal and external resources to assess fraud trends and define your future fraud strategy.

More than 250 professionals make up the team of the Center of Excellence in Fraud (CoE), specialised in the development and implementation of fraud programs for financial organisations **worldwide**.

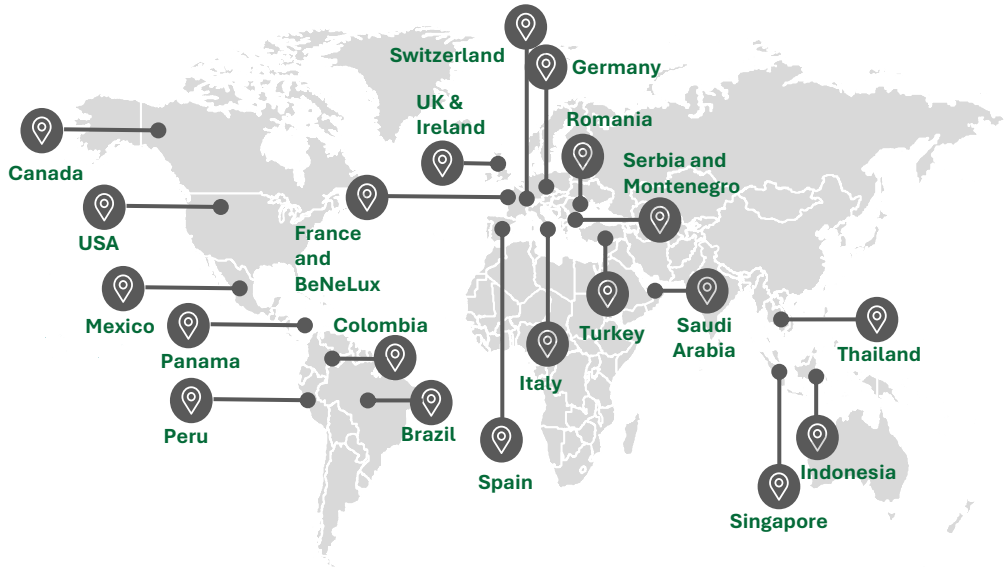
Since 2011, fraud professionals have been helping financial institutions **develop, implement and evolve their Fraud prevention and detection programs**

It is a multidisciplinary group of professionals that covers all areas of the implementation of fraud and financial crime prevention and detection programs, including technology development and integration, regulation, definition and functional support, security, solution calibration, maintenance and operation of systems.

Main competencies:

- **Advising** financial institutions to support fraud **programs** and anti-money laundering
- **Selection, implementation and calibration of technological solutions** for the prevention of Fraud
- **Continuous improvement** of fraud detection by providing **Fraud Intelligence services** and **advanced detection mechanisms**
- **Operation and maintenance** of technological solutions for Fraud

Deloitte's Fraud Centre of Excellence provides services globally:



Alliances with the most important fraud tool vendors

Sectoral initiatives:

- Since October 2021, Deloitte has been regularly organising the **Fraud Prevention Club in financial institutions**. It is a benchmark forum in fraud prevention attended by practically all those **responsible for fraud** in financial institutions. It is intended as a **forum of trust** and alert about potential fraud attacks in which **access to experts in the fraud and cybersecurity sector** is facilitated.

Deloitte.

Your contacts

Dr. Madan Sathe
Partner

+41 79 647 3151
msathe@deloitte.ch

Dr. Konrad Schwenke
Senior Manager

+41 79 535 1488
kschwenke@deloitte.ch

Deloitte.