Financial Crime Risks in the Digital Era

مخاطر الجرائم المالية في ظل العصر الرقمي

Ali Awartany

Consultant and Trainer

Head of Compliance and Risk Management Officer at MadfooatCom

PhD in Business Economics

Diverse banking experience in financial institutions (17 years)

12 years of experience as a consultant and trainer in compliance and risk management

CERTIFIED COMPLIANCE MANAGER
GLOBAL COMPLIANCE INSTITUTE

CAMS
Certified Anti-Money Laundering Specialist®

CFCS
CERTIFIED FINANCIAL CRIME SPECIALIST

ASQ
Certified Six Sigma Green Belt
The Global Voice of Quality™

CGSS
CERTIFIED GLOBAL SANCTIONS SPECIALIST

Data Science
MICROSOFT PROFESSIONAL PROGRAM

PMI
PMP
Certified

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS
CFE
CERTIFIED FRAUD EXAMINER

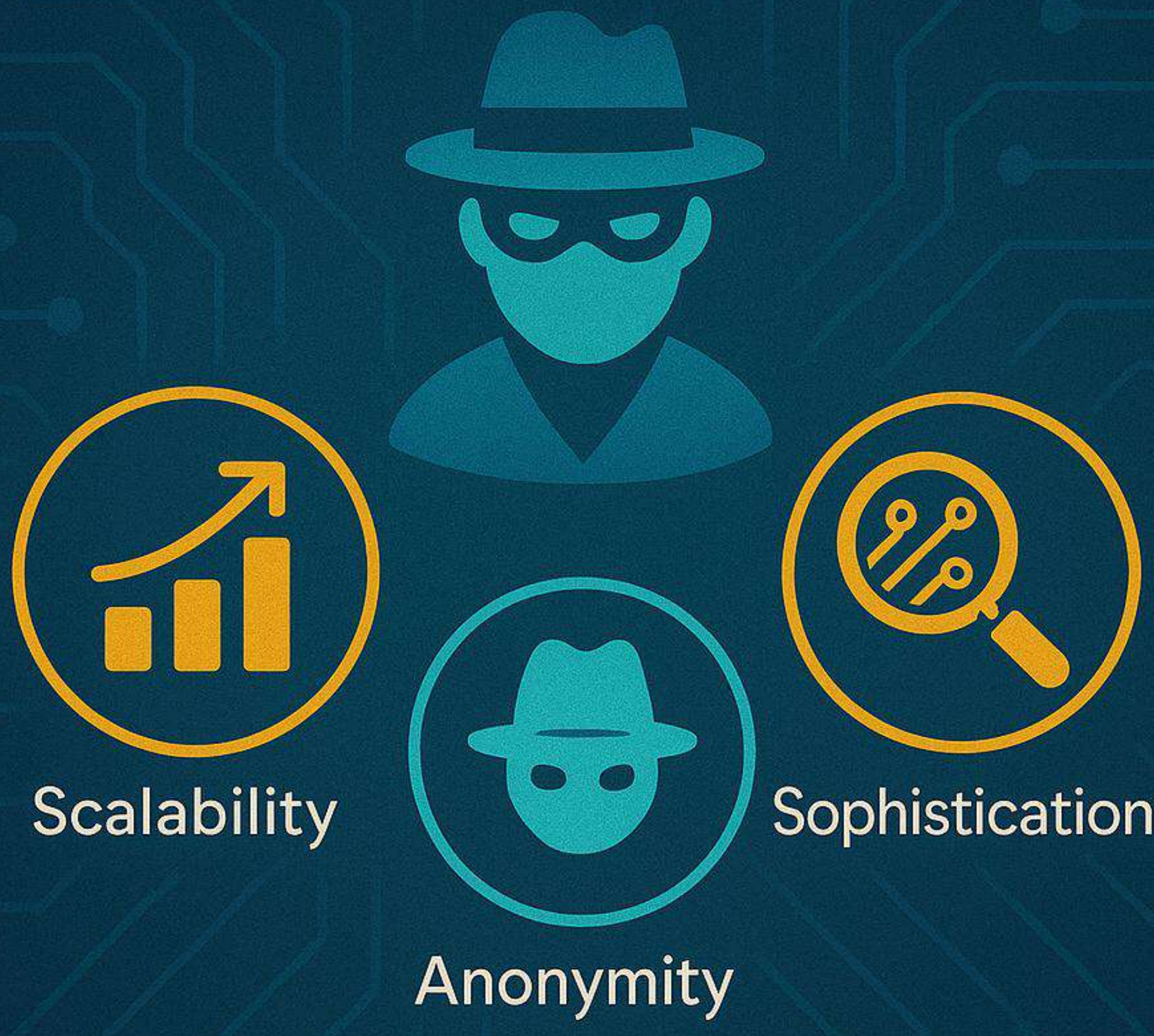
CIA®
Certified Internal Auditor®

Agenda

- Technology-enabled financial crime and emerging typologies.
- Digital onboarding, remote KYC, and fraud prevention challenges.
- Supervisory perspectives on digital compliance maturity.

Digital financial crimes refer to illegal activities carried out through digital channels, financial technologies, or electronic payment systems with the objective of stealing funds, manipulating transactions, or abusing financial services.

KEY CHARACTERISTICS



- **Exploitation of digital banking, payment platforms, wallets, cards, and online financial services.**
- **Abuse of customer data, credentials, and digital identities.**
- **Use of technology and automation to scale and conceal criminal activity.**
- **Scalability (fraud at speed and volume), anonymity (harder to trace), and sophistication (harder to detect).**

Global Scale of Financial Crime

- In 2023, it's estimated that **over $3.1 trillion** in illicit funds flowed through the global financial system. This includes money laundering, fraud, and other financial crimes.
- Of that, fraud scams and bank fraud schemes alone accounted for about **$485–$500 billion** in projected losses worldwide.

$3.1+ Trillion

IN ILLICIT FUNDS

Estimated to flow through the global financial system in 2023

$485–500 Billion

IN PROJECTED LOSSES

Fraud scams and bank fraud **worldwide**

Money Laundering Figures

- Between 2% and 5% of global GDP — which is roughly **$800 billion to $2 trillion** annually — is estimated to be laundered worldwide each year.
- Some reports show money laundering estimates of **over $1.6 trillion** per year, highlighting the massive scale across jurisdictions.

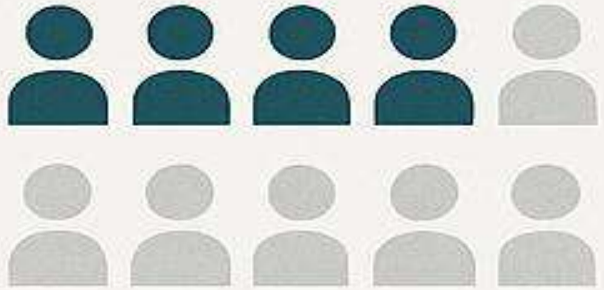
$800B to $2 Trillion

Laundered Each Year

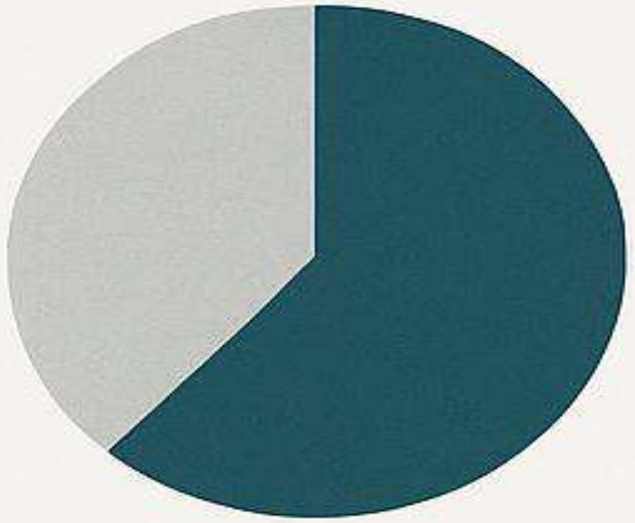
$800B to $2 Trillion

Laundered Each Year

In 2022, identity theft affected 1 in every 15 online transactions



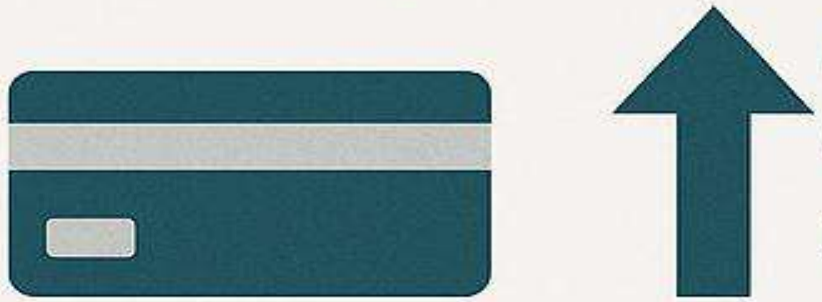
Friendly fraud accounted for 41% of all chargebacks in 2020



Phishing attacks represented 44% of all e-commerce fraud attempts in 2020

A 2024 survey of 20,000 employed adults revealed that nearly half had fallen victim to cyberattacks or scams, with 45% reporting compromised personal data

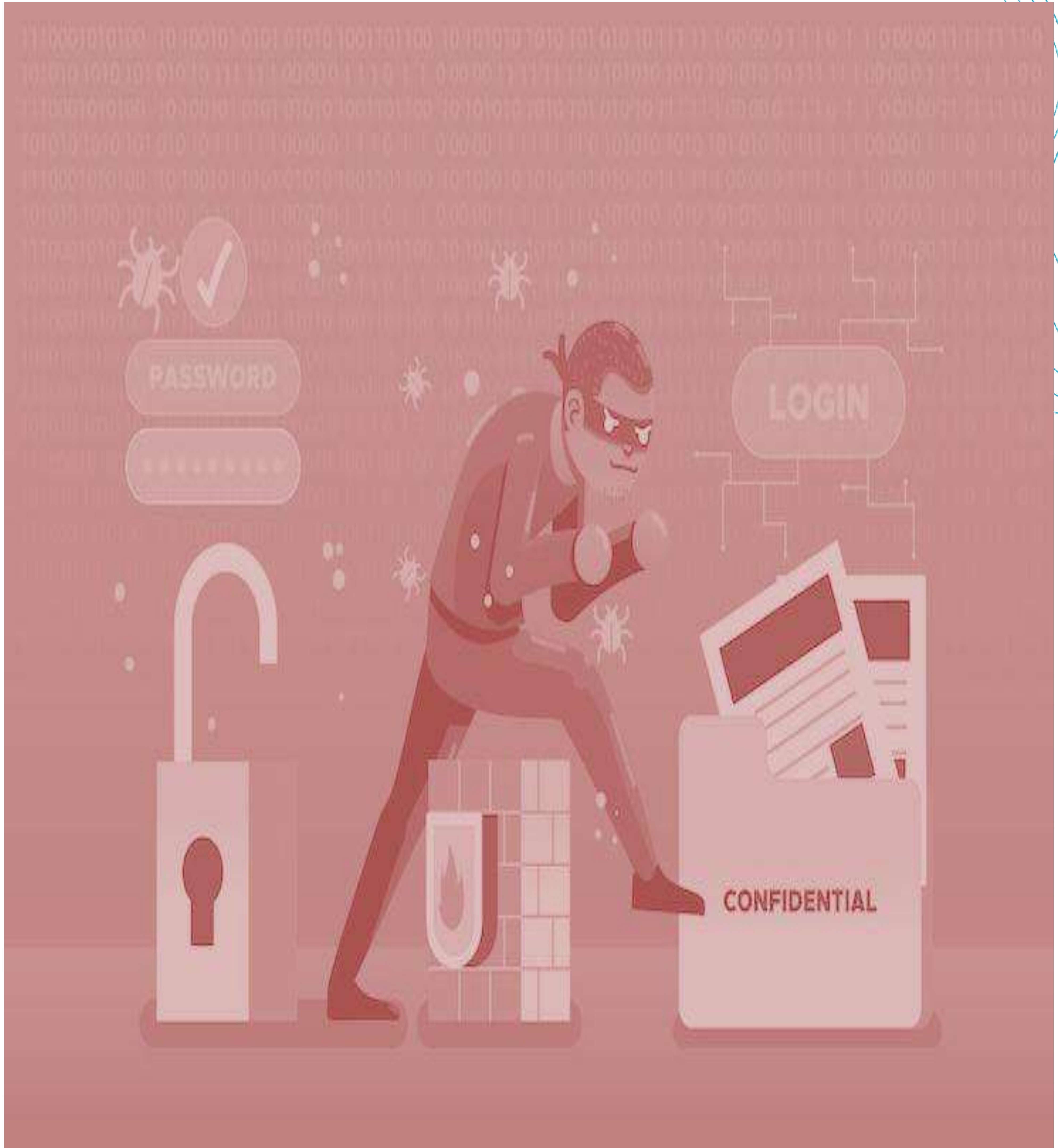
Card-not-present fraud is 81% more likely to happen than card-present fraud



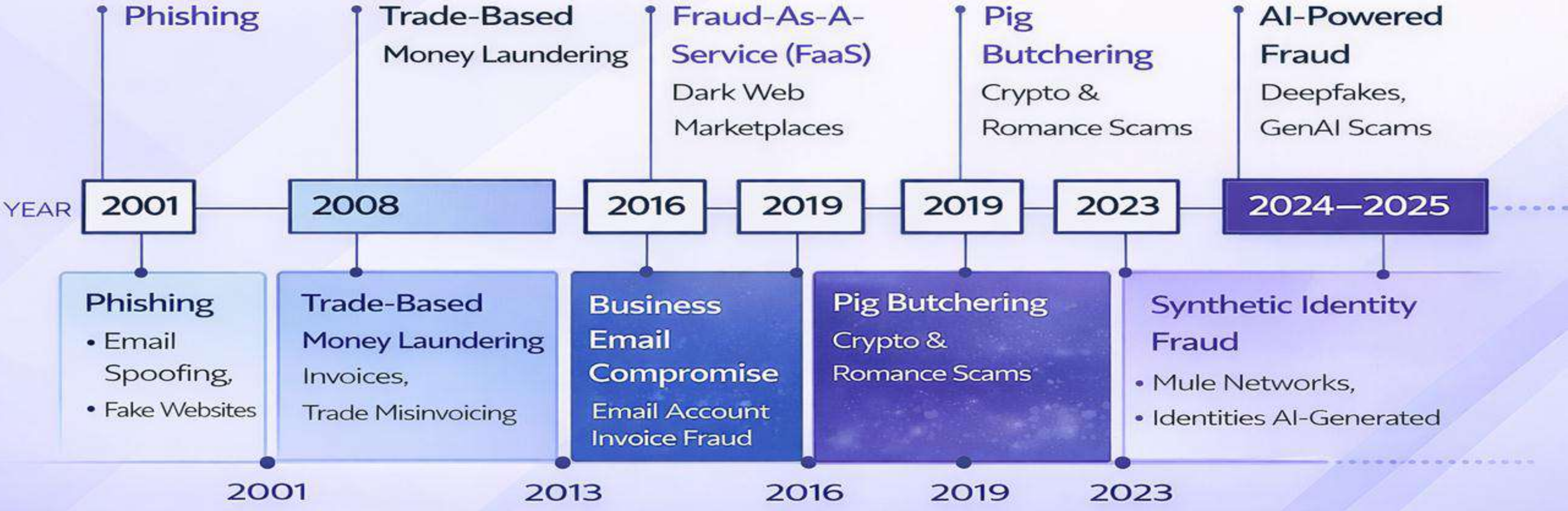
81% more likely

In 2025, analysts estimated that card-not-present fraud would nesult in nearly $9.5 billion losses, indicating an 8.5% increase from the previous year

Emerging Threats



Evolution Of Financial Crime Typologies



Phishing

Trade-Based Money Laundering

Fraud-As-A-Service (FaaS)
Dark Web Marketplaces

Pig Butchering
Crypto & Romance Scams

AI-Powered Fraud
Deepfakes, GenAI Scams

YEAR 2001 2008 2016 2019 2019 2023 2024—2025

Phishing

- Email Spoofing,
- Fake Websites

Trade-Based Money Laundering
Invoices,
Trade Misinvoicing

Business Email Compromise
Email Account
Invoice Fraud

Pig Butchering
Crypto &
Romance Scams

Synthetic Identity Fraud

- Mule Networks,
- Identities AI-Generated

2001 2013 2016 2019 2023

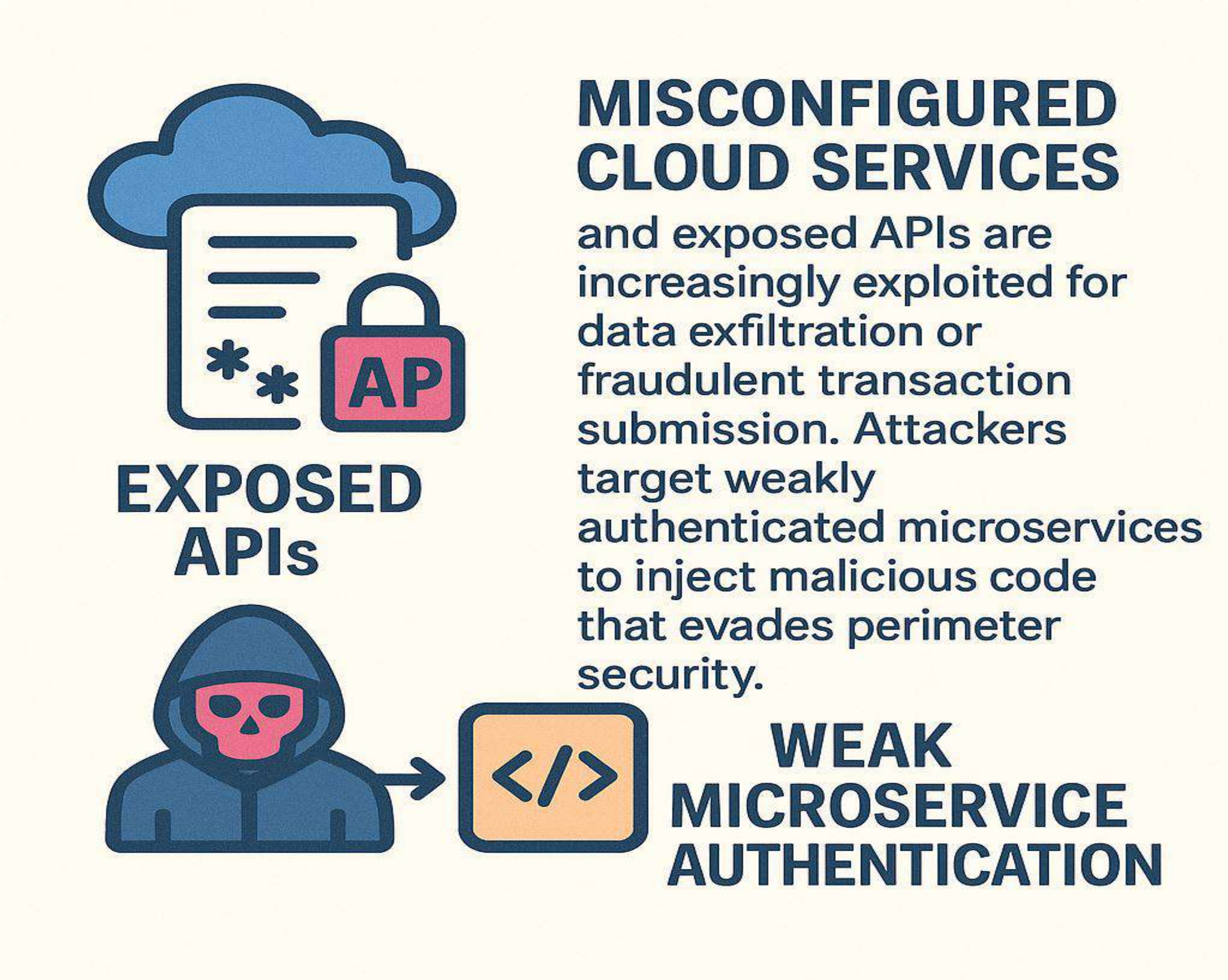
Technological Advances Enabling New Fraud Vectors

AI/ML-DRIVEN FRAUD AND DEEPFAKES
API
CLOUD-NATIVE AND API VULNERABILITIES
IoT AND DEVICE EXPLOITATION

AI-Enabled Deepfakes in e-KYC & Digital Onboarding

- Cybercriminals increasingly use AI and machine learning to create deepfakes — highly realistic fake videos, voice recordings, and images that can bypass traditional identity verification controls.
- Deepfakes are used to impersonate legitimate customers during remote account opening and e-KYC processes, exploiting weaknesses in:
    - Facial recognition
    - Liveness detection
    - Document verification
    - Video-based onboarding interviews
- A financial institution unknowingly onboarded multiple accounts after fraudsters used AI-generated faces and synthetic voices to pass video KYC and selfie-based verification, enabling the creation of mule and synthetic identity accounts that were later used for fraud and money laundering.

Cloud-Native and API Vulnerabilities

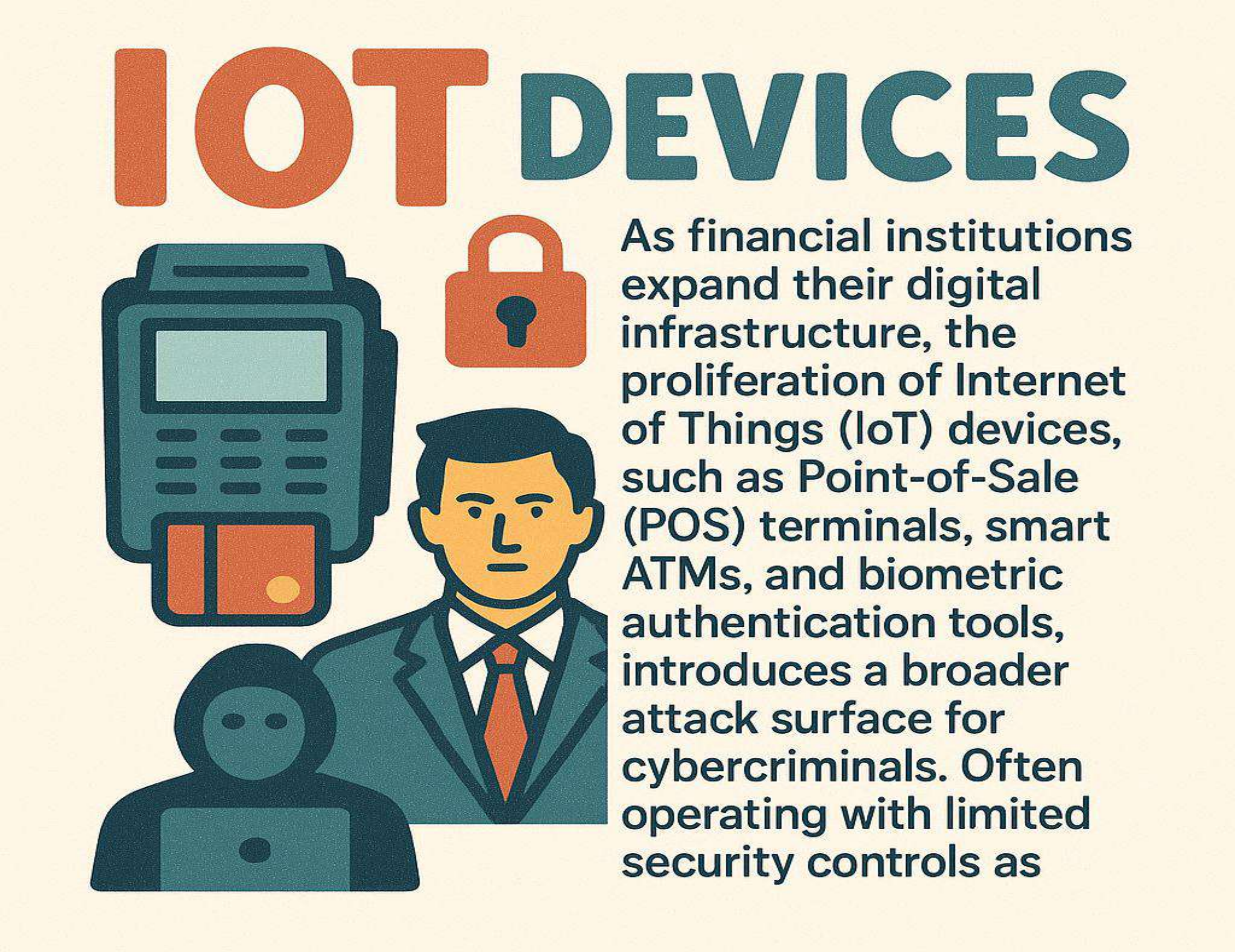


MISCONFIGURED CLOUD SERVICES and exposed APIs are increasingly exploited for data exfiltration or fraudulent transaction submission. Attackers target weakly authenticated microservices to inject malicious code that evades perimeter security.

Cloud-Native and API Vulnerabilities

- Hackers exploit misconfigured cloud systems and unsecured APIs to steal data or execute fraudulent transactions.
- Weak authentication in micro services can allow attackers to inject malicious code and bypass security controls.
- Strong configuration, API security, and robust authentication for micro services are critical to preventing breaches.

IoT and Device Exploitation



As financial institutions expand their digital infrastructure, the proliferation of Internet of Things (IoT) devices, such as Point-of-Sale (POS) terminals, smart ATMs, and biometric authentication tools, introduces a broader attack surface for cybercriminals. Often operating with limited security controls as

COMPROMISED IOT DEVICES CAN BE USED TO GAIN A FOOTHOLD AND INFILTRATE CRITICAL SYSTEMS

IoT and Device Exploitation

- Advanced replay attacks mimic users’ behavioral patterns (typing, gestures) to bypass mobile authentication.
- This challenges the effectiveness of continuous verification systems.
- Stronger, multi-layered authentication with real-time anomaly detection and device-level risk scoring is essential.

IoT and Device Exploitation

In response, financial institutions must:

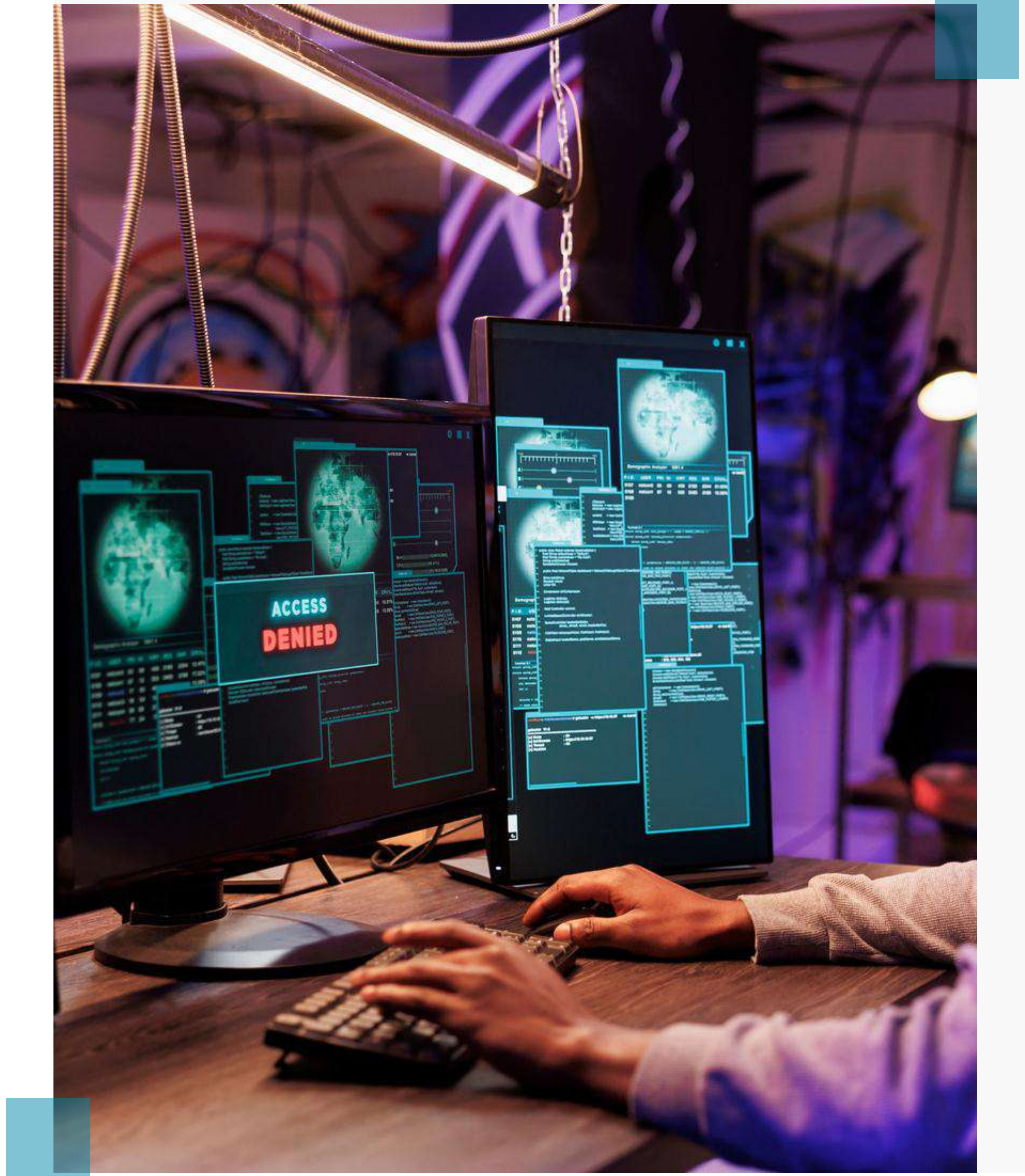
Regularly patch and monitor all connected devices.

Adopt AI-driven threat detection.

Segment IoT networks from core systems.

Ensure biometric authentication systems are equipped to detect spoofing or replay attempts.

Financial Crimes Detection & Prevention



AI-Powered Financial Crimes Detection & Prevention

- Artificial Intelligence (AI) and Machine Learning (ML) are revolutionizing financial crimes detection by identifying suspicious patterns, analyzing user behavior, and automating responses.

Predictive Analytics in Financial Crime Prevention

Predictive analytics uses historical and real-time data, machine learning, and behavioral patterns to **anticipate and prevent financial crime before it materializes**.

Applied Use Cases

- ✓ Early detection of fraud and account takeover
- ✓ Predicting suspicious transaction behavior
- ✓ Identifying high-risk customers and merchants
- ✓ Reducing false positives in AML monitoring

From reactive investigation → to proactive prevention

Predictive Analytics Life Cycle in Financial Crime

Financial Crime Analytics Life Cycle

- **Risk Definition** – Identify fraud / ML / TF / sanctions risk
- **Data Ingestion** – Transactions, devices, behavior, KYC
- **Feature Engineering** – Velocity, frequency, geolocation, patterns
- **Model Development** – Scoring, clustering, anomaly detection
- **Decisioning** – Approve | Alert | Block | Escalate
- **Monitoring & Feedback** – Model tuning & regulatory validation

Why this matters

➢ Aligns **business, compliance, IT, and analytics**

➢ Supports **regulatory explainability**

Predictive Models Used in Financial Crime

Core Predictive Models & Examples

Model Type	Financial Crime Application
Classification	Will this transaction be fraudulent?
Anomaly Detection	Is this behavior abnormal for this customer?
Clustering	Grouping mule accounts or fraud rings
Time-Series Forecasting	Anticipating fraud spikes (paydays, campaigns)
Risk Scoring	Customer / merchant / transaction risk score

Models must be **explainable, auditable, and bias-controlled**.

Where Predictive Analytics Fits in the Digital Risk Landscape

Digital Era Risk Coverage

Predictive analytics strengthens controls across:

- ✓ Mobile wallets & instant payments
- ✓ Open Banking & APIs
- ✓ E-commerce & QR payments
- ✓ Cross-border and correspondent flows

Digital growth without predictive analytics = **scaled risk**

The Three Pillars of Financial Crime Defense

Financial Crimes detection and prevention have evolved significantly with advancements in technology.

The ability to analyze **big data** has transformed how Financial Crimes analysts monitor customer behavior and transactions.

Three core pillars of Financial Crimes detection and prevention ensure a robust defense against criminal activities:

- ✓ **A Refined Rules Engine**
- ✓ **Machine Learning**
- ✓ **Link Analysis Using Graph Databases**

A Refined Rules Engine

Rules were the foundation of traditional detection systems before machine learning revolutionized the field.

While machine learning enhances prevention, rules remain crucial in specific scenarios.

When Are Rules Effective?

❑ **Rapid Response to Fraud Attacks**

- Analysts can quickly **block fraudulent activity** by setting location-based or behavioral rules.
- Example: **Blacklisting transactions from a known high-risk region.**

❑ **Addressing Emerging Fraud Trends**

- Machine learning models rely on historical data (often **3+ months old** due to delays).
- Analysts can use rules **proactively** to block **new patterns** before models adapt.

❑ **Combining Multiple Indicators**

Rules allow Financial Crimes managers to **layer conditions**, targeting specific behaviors.

Machine Learning: The Game-Changer in Fighting Financial Crimes

Machine learning processes vast amounts of **historical and real-time data** to identify risks dynamically.

How It Works

- ✓ **Risk Scoring**: Instead of simple yes/no rules, ML assigns risk scores (Low, Medium, High).
- ✓ **Automated Decision-Making**: Models analyze **thousands of transactions per second**, detecting fraud within **milliseconds**.
- ✓ **Pattern Recognition**: Detects **subtle fraud patterns** that human analysts or rule-based systems might miss.

Why Machine Learning is More Effective?

- ✓ Adapts to New Fraud Tactics
- ✓ Continuously Learns & Updates
- ✓ Works in Real-Time
- ✓ Minimizes Human Input While Maximizing Detection

Link Analysis: Uncovering Hidden Networks in Financial Crimes

Link analysis acts as a powerful investigative tool, visualizing and analyzing relationships among entities—such as accounts, transactions, individuals, and devices—to detect complex financial crime schemes.

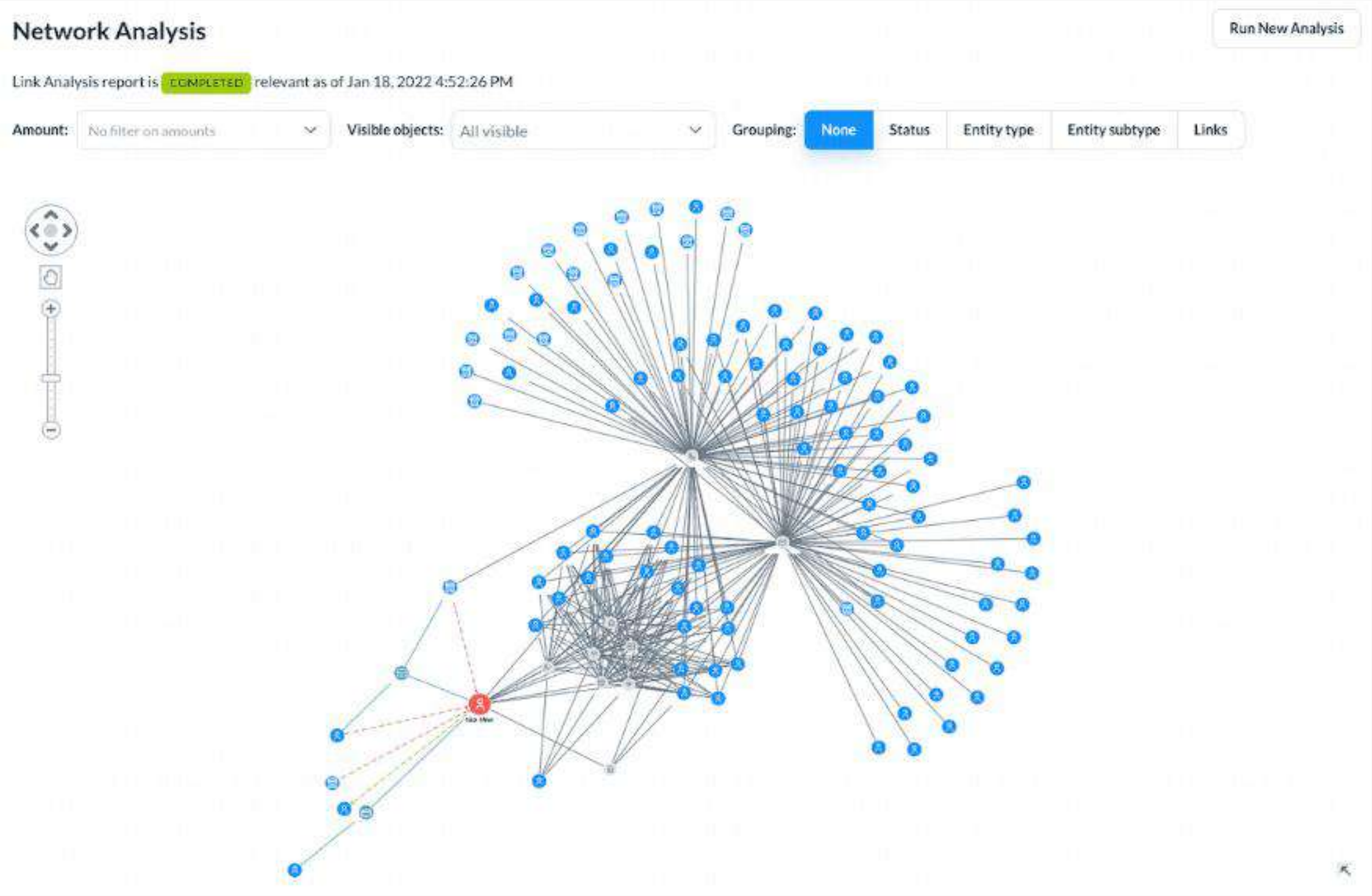
How Link Analysis Strengthens Financial Crime Detection

⍰ **Reveals Suspicious Connections**
Identifies indirect and hidden links between accounts, individuals, devices, and locations often missed by traditional monitoring.

⍰ **Uncovers Organized Criminal Networks**
Detects coordinated activity and large-scale schemes, including layering and structuring, by mapping transactional behavior across multiple entities.

⍰ **Enhances Machine Learning and Analytics**
Provides rich network data that improves the accuracy and predictive power of AI/ML models in identifying and flagging high-risk patterns.

Link Analysis: Uncovering Hidden Networks in Financial Crimes



Network Analysis

Link Analysis report is COMPLETED relevant as of Jan 18, 2022 4:52:26 PM

Amount: No filter on amounts

Visible objects: All visible

Grouping: None

The Role of Predictive Analytics in Fighting Financial Crimes

Predictive analytics enhances fraud prevention by forecasting financial crimes risks based on past behaviors.

Key Strengths of Predictive Analytics

✓ **Continuous Learning** – Adapts to evolving fraud tactics.

✓ **Anomaly Detection** – Flags unusual user behavior.

✓ **Adaptable Models** – Adjusts based on new fraud trends.

✓ **Contextual Analysis** – Provides deeper insights into fraudulent activities.

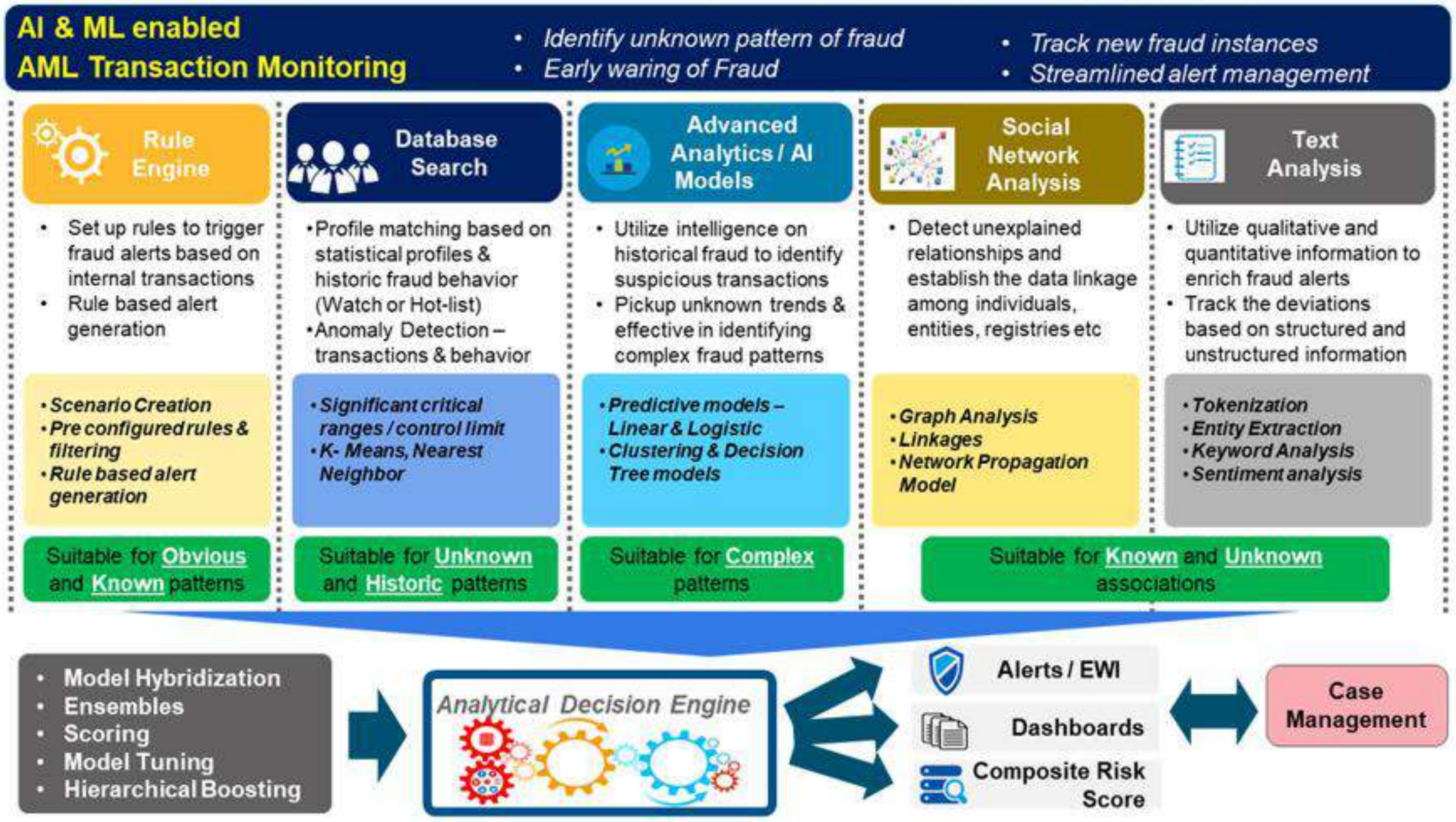
A Multi-Layered Defense Against Financial Crimes

✓ Rules + Machine Learning + Link Analysis create a strong prevention strategy.

✓ Machine learning enhances efficiency, while rules and link analysis provide targeted, proactive prevention.

✓ A data-driven, adaptive approach ensures criminals stay one step behind.

A Multi-Layered Defense Against Financial Crimes



AI & ML enabled AML Transaction Monitoring

- *Identify unknown pattern of fraud*
- *Early waring of Fraud*
- *Track new fraud instances*
- *Streamlined alert management*

Rule Engine

- Set up rules to trigger fraud alerts based on internal transactions
- Rule based alert generation

- *Scenario Creation*
- *Pre configured rules & filtering*
- *Rule based alert generation*

Suitable for Obvious and Known patterns

Database Search

- Profile matching based on statistical profiles & historic fraud behavior (Watch or Hot-list)
- Anomaly Detection – transactions & behavior

- *Significant critical ranges / control limit*
- *K- Means, Nearest Neighbor*

Suitable for Unknown and Historic patterns

Advanced Analytics / AI Models

- Utilize intelligence on historical fraud to identify suspicious transactions
- Pickup unknown trends & effective in identifying complex fraud patterns

- *Predictive models – Linear & Logistic*
- *Clustering & Decision Tree models*

Suitable for Complex patterns

Social Network Analysis

- Detect unexplained relationships and establish the data linkage among individuals, entities, registries etc

- *Graph Analysis*
- *Linkages*
- *Network Propagation Model*

Text Analysis

- Utilize qualitative and quantitative information to enrich fraud alerts
- Track the deviations based on structured and unstructured information

- *Tokenization*
- *Entity Extraction*
- *Keyword Analysis*
- *Sentiment analysis*

Suitable for Known and Unknown associations

- Model Hybridization
- Ensembles
- Scoring
- Model Tuning
- Hierarchical Boosting

Analytical Decision Engine

Alerts / EWI

Dashboards

Composite Risk Score

Case Management

What Supervisors Mean by “Digital Compliance Maturity”

Key supervisory perspective:

Digital compliance maturity reflects how effectively an institution embeds technology, governance, and risk intelligence to manage financial crime risks in a digital environment.

From a regulator’s lens, maturity is about:

- ✓ Effectiveness, not just technology adoption
- ✓ Risk-based, proportionate controls
- ✓ Ability to prevent, detect, and respond in near real time
- ✓ Strong governance and accountability, even with automation

Supervisors are not asking:

“Do you have a system?”

They are asking:

“Does your system actually work — and can you prove it?”

Digital Compliance Maturity: What Supervisors Look For

Supervisory expectations typically focus on 4 pillars:

Governance & Ownership

- Clear accountability for digital AML/CFT & fraud systems
- Board and senior management oversight

Risk-Based Design

- Controls aligned with actual digital risks (e-wallets, APIs, instant payments)
- Differentiation between low, medium, and high-risk users/transactions

Data Quality & Integrity

- Reliable, complete, and explainable data inputs
- Controls over data lineage, accuracy, and timeliness

Monitoring, Alerts & Escalation

- Real-time or near real-time monitoring where required
- Clear alert logic, escalation paths, and decision accountability

During inspections, supervisors typically ask:

Design

- Why were these rules, thresholds, or models selected?
- How do they reflect your digital business model?

Operation

- Are alerts meaningful or just high volume?
- Are decisions consistent and documented?

Effectiveness

- Can you demonstrate detection of real cases?
- How do you measure false positives vs missed ritsks?

Adaptability

- How fast can controls be updated for new risks?
- How did you respond to the last fraud/AML incident?

Evidence

- Policies, logs, dashboards, tuning records, audit trails
- Not verbal explanations — **documented proof**

Key Takeaways

- ❑ Financial crime is data-driven and fast-moving
- ❑ Predictive analytics enables early intervention
- ❑ Success requires technology + governance + skilled people
- ❑ Regulators increasingly expect advanced analytics maturity
- ❑ In the digital era, supervisors don’t supervise systems —
  they supervise how institutions govern, control, and explain them

THANK YOU

Compare
Indicator
Template
Snap
Save
Idea
85%
Brainstorm
50%
Analysis
30%
Plan
18%
Start
5%