# Forward thinking in fraud strategy: the generative AI and agentic AI advantage

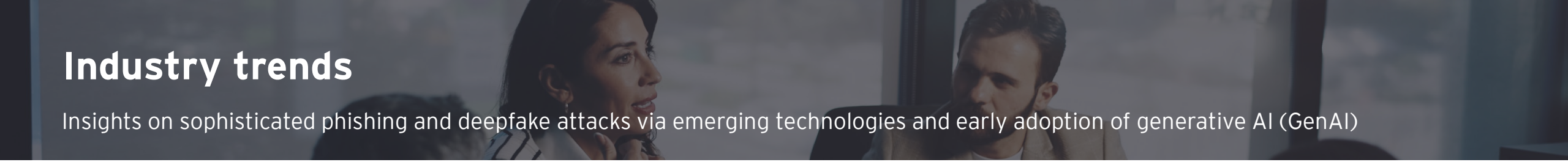
2025

The better the question. The better the answer. The better the world works.

Shape the future with confidence

# Disclaimer

- The views expressed by the presenters are not necessarily those of Ernst & Young LLP or other members of the global EY organization.
- These slides are for educational purposes only therefore are not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.



# Industry trends

Insights on sophisticated phishing and deepfake attacks via emerging technologies and early adoption of generative AI (GenAI)

## AI phishing

**60%** of recipients fall victim to artificial intelligence (AI)-generated phishing emails, same as non-AI-made emails[1]

Scammers save **95%** in costs by using large language models (LLM) to create phishing emails[1]

## AI deepfakes

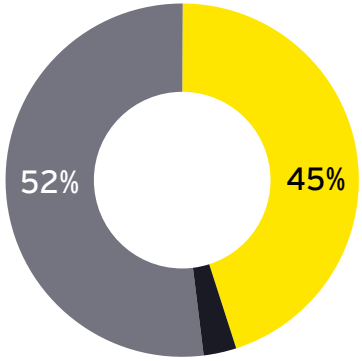
Deepfake attacks were forecast to rise **50%** to **60%** in 2024 to 140,000 to 150,000 globally[2]

Impersonation scams cost US victims **$12.5b** in losses in 2023[3]

## Institutions are actively exploring GenAI initiatives

**52%**

of institutions are planning to invest or are highly interested in learning more

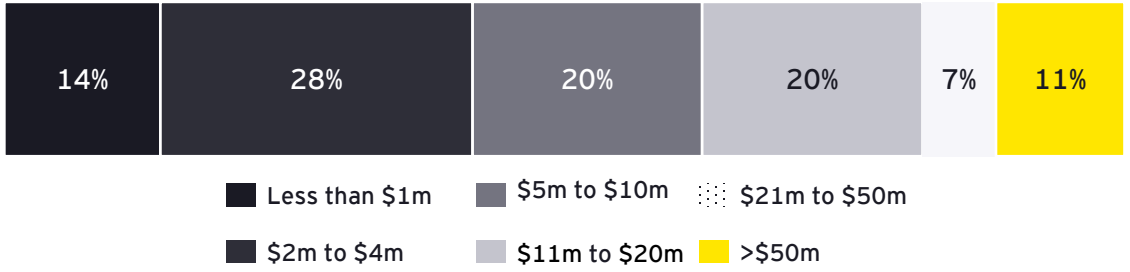



**45%**

of institutions are already investing in GenAI, mostly ideating or experimenting

Source: EY Parthenon

## And have begun making investments in dedicated GenAI teams to realize these benefits

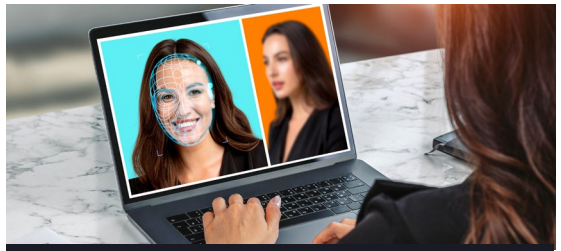



Funding amounts largely **correlate with institution segment sizes**, with most spending <20% of their budget on GenAI

Source: EY Parthenon

[1]https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams
[2]https://venturebeat.com/security/how-ai-driven-identity-attacks-are-defining-the-new-threatscape/
[3]https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

# Evolving fraud schemes fueled by GenAI

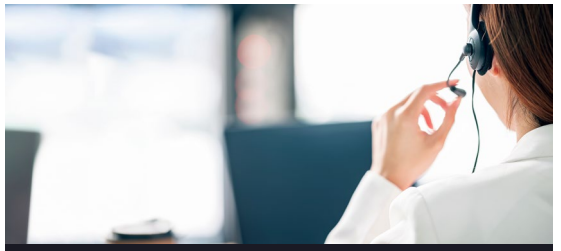


## Deepfakes

- **Mimic**, replace or alter a real **person's likeness.**
- **AI mimics** an executive's **voice to instruct** internal employees to execute funds transfers.
- Red flags include secrecy, urgency, or an unusual nature of the request.


## Fraud-as-a-Service

- Bad **actors provide tools, services and expertise** to carry out fraud on behalf of paying clients.
- **Fraud-as-a-Service** offering includes online payment fraud, account takeover, refund fraud and account farming.
- Encrypted apps and the dark web make it easy for **criminals to build a network** and communicate.



## Scams

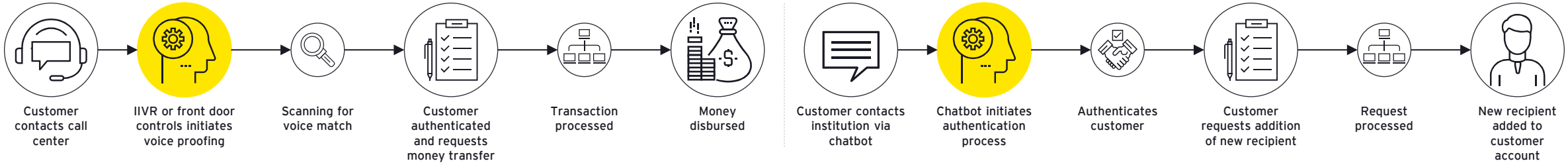
- Firms are seeing a **variety of scams** with investment scams, romance scams, government, and financial firms scams all **on the rise**.
- Occurs **across multiple channels, activities, and pathways.**
- Call spoofing, social engineering, data mining, predictive algorithms and other methods **increasingly use technology in sophisticated ways**.

## Synthetic identity

- Create a **fake identity** through a combination of real and fake personal information.
- **Play the "long game"** by slowly building a credit history until they eventually do a "bust out" on the established credit line.
- Increasing **data breaches due to a shift toward remote payment channels** and **inadequate identity verification** systems.

# Example of a GenAI-based fraud attack

Voice cloning and behavioral mimicry allow fraudsters to impersonate legitimate customers, bypassing traditional security measures




## Contact center fraud exploitation tactics and challenges

### Voice cloning (call)

Fraudsters can replicate the voices of customers or executives using GenAI

**Misuse in fraudulent activities**

Fraudsters might use cloned voices to bypass voice biometrics and authenticate fraudulent transactions, change account information, or gain unauthorized access to sensitive data

### Behavioral mimicry (chatbot)

Scammers mimic user behaviors (e.g., tones, language, vocabulary, knowledge, etc.) to evade detection systems

**Misuse in social engineering**

Scammers employ behavioral mimicry to bypass advanced security protocols that rely on behavior analysis to flag unusual activities

### Operational and security challenges

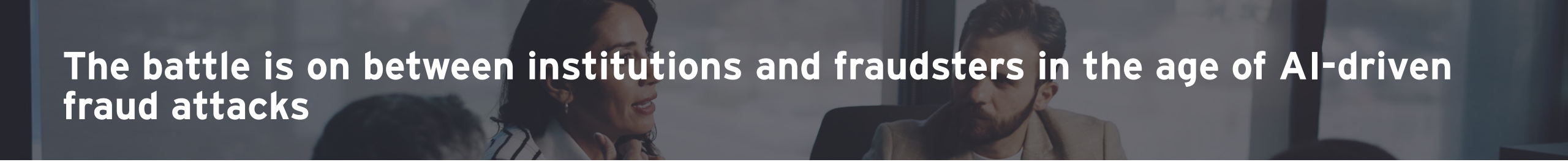
Institutions need to invest in more advanced detection systems that can differentiate between genuine and AI-generated interactions

### Impact on customer trust

Misuse of voice cloning and mimicry to facilitate breaches in personal information and transactional damages customer trust and data security

### Regulatory and compliance implications

Strict compliance with evolving digital security laws is crucial to avoid legal repercussions and maintain operational integrity



# The battle is on between institutions and fraudsters in the age of AI-driven fraud attacks

Fraudsters have deployed GenAI to launch sophisticated attacks. In response, institutions mostly rely on traditional AI/machine learning (ML) and enhanced legacy controls with limited or early adoption of GenAI-augmented tools, which falls short against these threats.

## Fraud vectors (GenAI)

**Deepfakes:**
Hyper-realistic fake videos are used for impersonation, scams and misinformation

**Synthetic identities:**
AI-generated personal information is utilized to create fake accounts/pass Know Your Customer (KYC) checks

**Voice cloning:**
Fraudsters mimic real voices for social engineering attacks and fraudulent activities

**Phishing emails:**
Highly personalized and grammatically accurate messages are generated at scale to deceive recipients

**Fake documents:**
AI-assisted document forgery is employed to create fake documents such as business records and passports

## Institutional response

**AI/ML models:**
Behavioral anomaly detection. Risk scoring based on transaction patterns. Historical fraud model training

**Enhanced legacy controls**
Identity verification, multi-factor authentication (MFA), device fingerprinting and geolocation checks IP unapproved-listing and velocity rules

**Hybrid fraud operations (automated and analyst-driven)**
Blend of automation and human expertise to manage fraud reviews, investigations, and deliver customer support through service centers

**Early adoption of GenAI-augmented tools**
Limited use of GenAI for alert triage and investigation summaries. Compliance documentation and report generation

## Challenges with institutional response

**High-friction** customer experiences persists **with limited personalization** and conversational fraud resolution

Fraud **controls are mostly reactive**, not real-time, and **fail to adapt** to AI-powered tactics

**Feedback** from fraud outcomes is rarely looped back **for learning**

**GenAI** is used in isolated tasks, **not embedded into workflows**

**Decision-making is fragmented** across siloed systems/channels

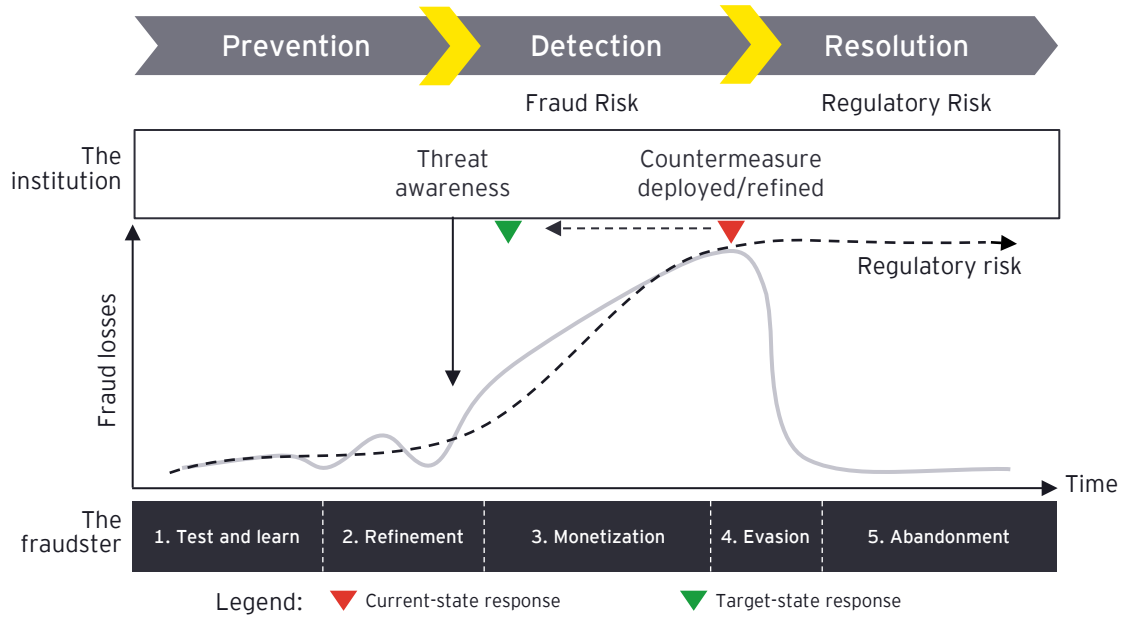
Heavy reliance on analysts creates **response delays with limited autonomous agents** to handle repeatable fraud ops tasks

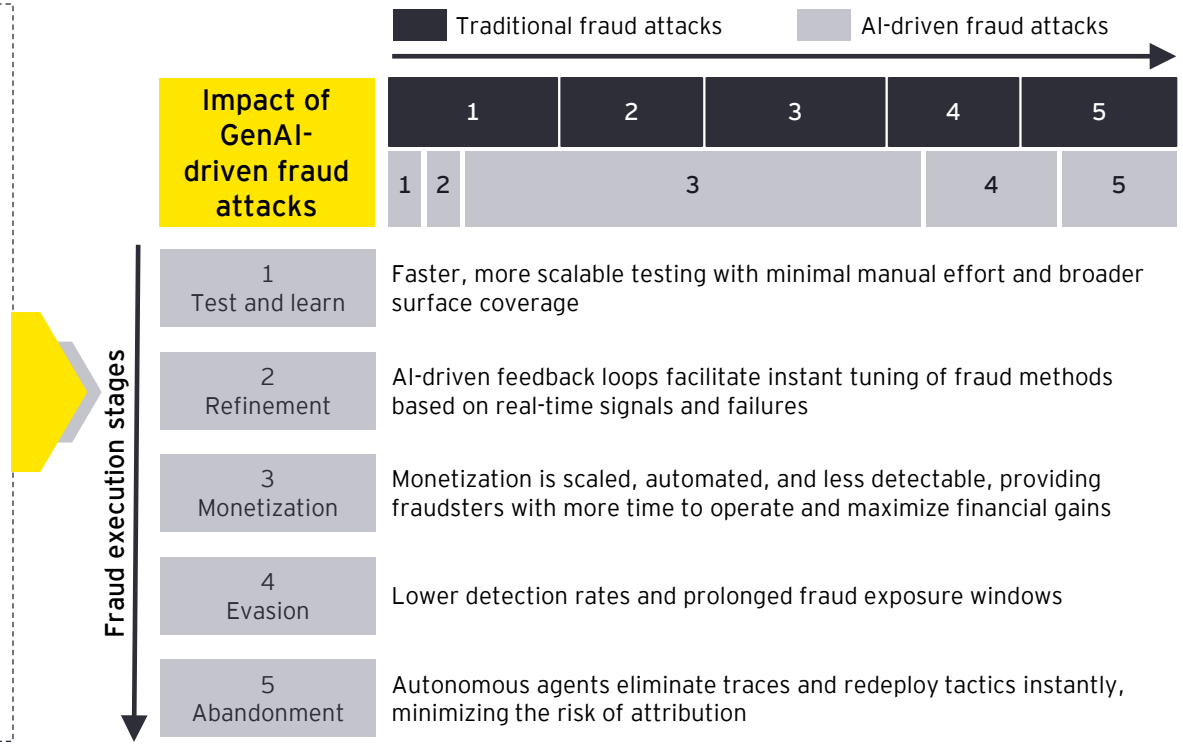
# Adopting GenAI capabilities for fraud risk mitigation is not a question of "why?" but "when?"

ILLUSTRATIVE

Accelerated testing and refinement enabled by AI allow fraudsters to initiate monetization earlier. Meanwhile, advanced evasion techniques and rapid abandonment strategies reduce the likelihood of detection and traceability

## Fraud execution stages and institutional response




This shift necessitates that the industry accelerate the adoption of GenAI and agentic AI solutions to stay ahead of evolving fraud tactics, focusing on enhancing control effectiveness, customer experience and operational efficiency

# Modernizing anti-fraud capabilities through adoption of GenAI and agentic AI

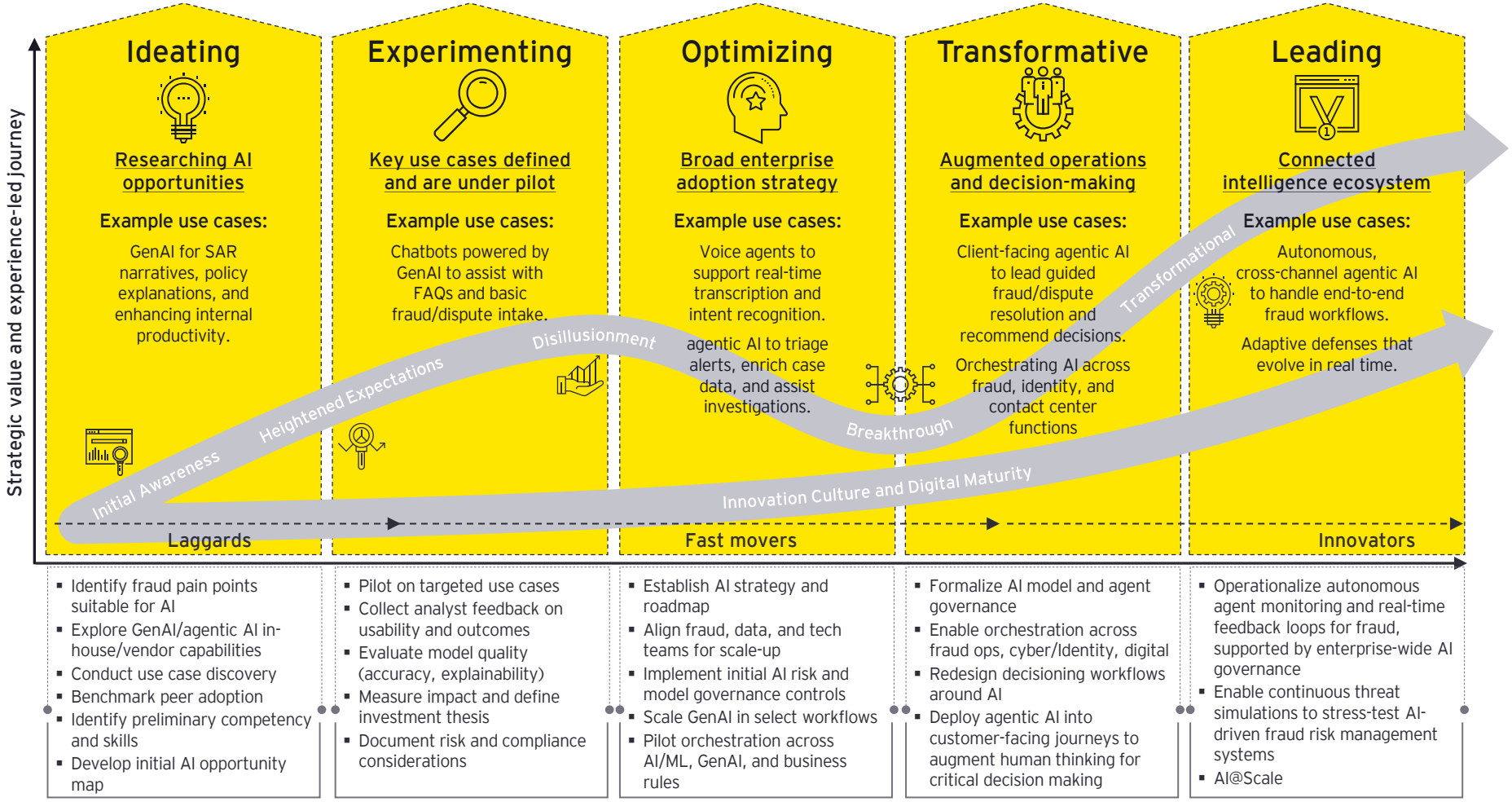
While institutions are realizing benefits from traditional AI, there is a much larger potential to be unlocked by adopting GenAI and agentic AI


| Traditional AI | GenAI and agentic AI |
|---|---|
| **Self-serve capabilities** | |
| Limited chatbots with scripted flows | Autonomous, guided self-resolution across channels |
| **Personalized communication** | |
| Pre-set personalization, lacks real-time context | Context-aware, user-specific responses in real time |
| **Omnichannel continuous experience** | |
| Fragmented experiences with repetitive interactions | Seamless, continuous journeys across channels and interactions |
| **Real-time, risk-based and adaptive controls** | |
| Point-in-time controls with limited real-time response | Dynamically adjusts controls using real-time risk signals |
| **Threat intelligence** | |
| Limited ability to simulate or adapt to external threats | Supports autonomous red teaming and simulation of evolving AI-driven tactics |
| **Cross-channel correlation** | |
| Channel-specific detection with limited linkage | Unified fraud signals across sessions, devices, and channels |
| **Workflow automation** | |
| Manual handoffs, static routing, rule-based task flows | Autonomous triage, escalation, and end-to-end workflow orchestration |
| **Enhanced investigative analysis** | |
| Manual data gathering, static summaries, siloed insights | Augments investigations with auto-context, dynamic insights, and summarization for faster resolution |
| **Continuous feedback and optimization** | |
| Static workflows and periodic tuning | Auto-refine fraud ops controls, processes and analyst performances in real time |

# Moving up the AI maturity curve to outpace competition and fraudsters

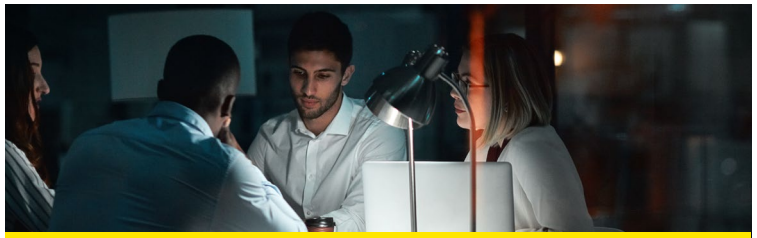
Most institutions are currently in the ideation or experimentation phase with GenAI and agentic AI for fraud risk management, with significant work needed to fully realize their potential and drive impactful results

| Maturity level | Definition |
|---|---|
| Leading | Fully autonomous, adaptive AI-driven fraud ecosystem with continuous learning |
| Transforming | AI is embedded across fraud operations with real-time orchestration and decision support |
| Optimizing | Scaling AI in select workflows and aligning fraud ops, tech, and data teams |
| Experimenting | Running pilots or PoCs for specific fraud workflows using GenAI/agentic AI |
| Ideating | Exploring AI opportunities to enhance the experience, effectiveness of fraud controls, and operational efficiencies |



# Areas institutions should consider for GenAI and agentic AI enablement

Key questions institutions who are ideating or experimenting GenAI and agentic AI adoption are trying to answer



## How do we leverage firm's existing technology and organizational assets?

- Enterprise platform availability
- Access to technical talent and business subject matter resources
- Governance and risk framework readiness

## How do we assess, prioritize and sequence the right use cases to create momentum?

- Business impact vs. implementation complexity
- Logical grouping and phasing of use cases
- Suitability of tasks for automation

## Where can we start now for initial prototyping and beta user evaluation?

- Leverage tech capability for rapid prototyping
- Put things in hands of users for evaluation
- Gather feedback and refine

**Should we automate today's processes or reimagine what's possible and redefine how things are done?**

# Prioritizing GenAI and agentic AI use cases by value and cost

ILLUSTRATIVE

## Prioritization lens for GenAI use cases

**Business value**

### Alignment to strategy/chosen archetypes

Evaluate the viability and impact of the use case on overall strategy and journey toward chosen archetype

### Enterprise usability

Prioritize enterprise-wide clusters of value, that can provide wide value-reach and realize cross-business unit synergies

### Probability of achieving predicted value

Success probability and predicted value are crucial guideposts for AI use case prioritization.

**Cost to build**

### Financial impact and value to customer

Evaluate the cost to build in the context of the value provided to the customer and impact on top line metrics

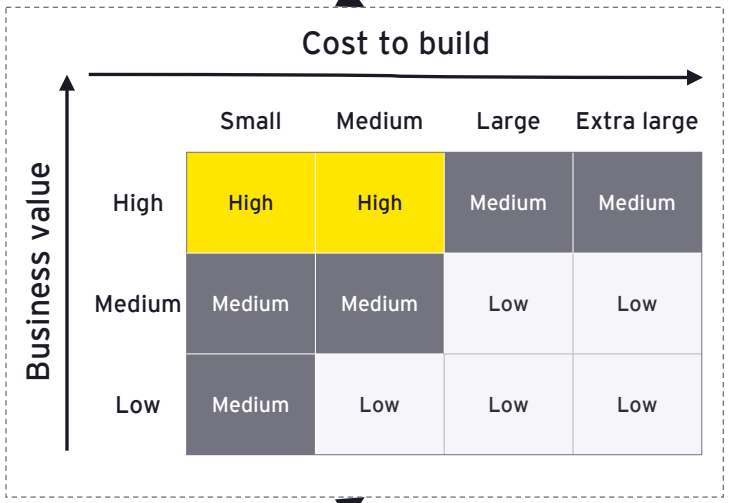
### Model risk

At maturing AI organizations, low-risk models should be prioritized until fairness evaluation frameworks are put in place

### Data maturity and implementation complexity

Factors such as data availability/maturity, model type, and intricacies of the business problem can raise development costs

- Alignment to strategy/chosen archetypes
- Enterprise usability
- Probability of achieving predicted value
- Financial impact and value to customer
- Model risk
- Implementation complexity




## Type of prioritized GenAI use cases

High and low value

- Use cases that drive clusters of value across the enterprise
- Quick-win use cases
- High-value, Business function specific use cases
- Transformational efforts with high value
- Niche use cases which can be low priority

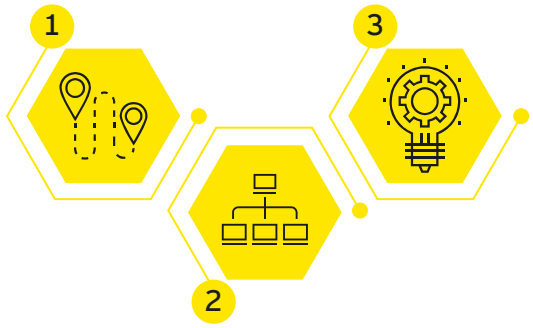
# Three critical for successful adoption of GenAI and agentic AI solutions for fraud risk management

## 3 critical phases for success

### GenAI strategy and roadmap

Deploy a roadmap for value creation through business or operating model transformation balancing risk and reward

- AI strategy
- Vendor analysis and technology selection
- Benefits realization framework
- Business case
- Diagnostics and use case selection
- Risk planning
- Target operating model design
- Roadmap and execution plan




### Governance and responsible AI

Establish processes, procedures, and enable model risk management

- AI/ML policy
- Model Validation Procedures/Standards
- AI Fairness/Bias Framework
- Heightened Risk Procedures
- Model Validation
- Ongoing Monitoring
- Benchmarking
- Model Change Management

### Scaled use case enablement

Prototype, build, scale and deliver use-cases into a full production environment (data ops, ML ops, API integration)

- Conceptual Design and Prototyping
- Process Design
- AI Model Build and Testing
- Performance Evaluation
- Technology/Infrastructure Build
- Ongoing Monitoring
- Model Change Management
- Leverage CoE use-cases

## Potential roadblocks

| | |
|---|---|
| 1 | **Organizational readiness** and **talent** gaps |
| 2 | **Data constraints** – quality, privacy, security and compliance concerns |
| 3 | Siloed, fragmented **legacy systems** and tools with limited visibility and integration capabilities |
| 4 | **Vendor lock-in** and tech stack misalignment |
| 5 | **Model risk** and **governance** challenges |
| 6 | **Ethical** and **customer trust** considerations |

# Ernst & Young LLP (EY US) fraud and AI team

## Fraud Strategy and Technology

**Robert Mara**
Principal
robert.mara@ey.com

**Aaron J. Glover**
Managing Director
aaron.j.glover@ey.com

**Dinesh Kumar Reddy**
Senior Manager
dinesh.kumar.reddy@ey.com

**Prasraban Mukhopadhyay**
Manager
prasraban.mukhopadhyay@ey.com

## Advanced Analytics and AI

**Sameer Gupta**
Principal
sameer.gupta@ey.com

**Sandeep Kumar**
Partner
sandeep.kumar3@ey.com

**John Radecki**
Principal
john.radecki@ey.com

**Ran Zhou**
Senior Manager
ran.zhou@ey.com

**Somnath Mukherjee**
Senior Manager
somnath.mukherjee@ey.com

## EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.



US SCORE no. 27168-251US
2505-10791-CS
ED None



ey.com