Unmasking elder fraud: how data and analytics can protect vulnerable customers

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

EY

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 and are not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

Table of contents

Case study 1: exploitation of a 75-year-old woman through romance scams and celebrity impersonation

Background information:

Mary lives in a suburban neighborhood and is an active user of social media platforms. Mary spent much of her time on her computer; she sought entertainment and friendship online, which made her susceptible to scams. The rise of romance scams, especially those involving impersonation of celebrities, has targeted many elderly individuals, in some cases leading to significant financial losses.

Findings:

Mary was approached on social media by an individual claiming to be a famous actor. The scammer built a rapport with her over several weeks, using fake profiles and photos to create a believable persona. The scammers leveraged AI and created deep fake videos, taken from the real actor's social media account to interact with Mary. She even claimed to have spoken to her suitor "for hours" on a chat platform. The following key points summarize the findings:

01 **Social media engagement:**
The scammer used social media to initiate contact, gaining Mary's trust through flattery and shared interests.

02 **Celebrity impersonation:**
The impersonation of a well-known actor added credibility to the scam, making Mary more susceptible to manipulation.

03 **Romance scams:**
After establishing a relationship, the scammer expressed a desire to marry Mary, further deepening her emotional investment.

04 **Funding the scam:**
As Mary expressed a lack of funds, the scammer was able to leverage months of knowledge through his "courtship" of Mary to identify her faith in psychics, mediums and guides. Mary received unsolicited attention from various individuals who sold her readings that indicated when she would be coming into a large sum of money.

05 **Methods of money movement:**

- Gift cards: Mary was instructed to purchase gift cards and send the codes to the scammer as "proof of her love" and to cover various fictitious expenses.
- Wire transfers: the scammer requested wire transfers to cover supposed legal fees related to their upcoming marriage.
- Compromised account credentials: Mary unknowingly provided her bank account information, which the scammer used to withdraw funds.
- New lines of credit: the scammer encouraged Mary to open new credit lines to fund their relationship, leading to maxed-out credit cards.
- Cash withdrawals: Mary withdrew cash from her savings to send to the scammer, believing it was necessary for their future together.

06 **Emotional manipulation:**
The scammer frequently used emotional tactics, claiming to be in danger or needing urgent financial help, which pressured Mary into complying with their requests.

Case study 2: exploitation of an elderly individual through a computer support impersonation scam

Background information:

In 2023, a Connecticut resident became the victim of a sophisticated tech support scam that began with a pop-up alert on their computer, falsely claiming their system had been compromised. The scam involved fraudsters posing as technical support agents and, later, government officials. Over time, they convinced the victim that their financial assets were at risk and needed to be secured by withdrawing large amounts of cash. The scammers manipulated the victim into physically mailing cash to various addresses across the United States.

Fortunately, one of these packages – containing $18,000 – was intercepted by federal authorities at a courier facility in New Jersey. A broader investigation led to the recovery of a total of $328,573, which was successfully returned to the victim.

Findings:

A Connecticut resident was defrauded of over $300,000 through a complex, multi-layered scam. The fraud involved technical manipulation, impersonation of legitimate institutions and high-pressure emotional tactics.

01 **Tech support pop-up scam:**
The scam started with a fake security pop-up claiming the victim's computer was compromised and urging them to call a support number.

02 **Impersonation of tech support and remote access:**
The victim called the number, connecting with fraudsters posing as IT support. The scammers gained remote access to the victim's device and escalated the fear by simulating financial threats.

03 **Government impersonation:**
The fraudsters posed as federal agents, urging the victim to withdraw and mail cash to protect their assets from "seizure." This built legitimacy and increased the pressure.

04 **Funding the scam:**
The victim was told a wire transfer was the only means to "secure" their accounts. This was a pivotal manipulation tactic that raised suspicion, prompting the victim to report the losses and led to involvement by law enforcement.

05 **Methods of money movement:**
The victim was told that wiring her money was the only way to "secure" it. She sent two large wire transfers totaling $550,000, believing it was a protective measure.

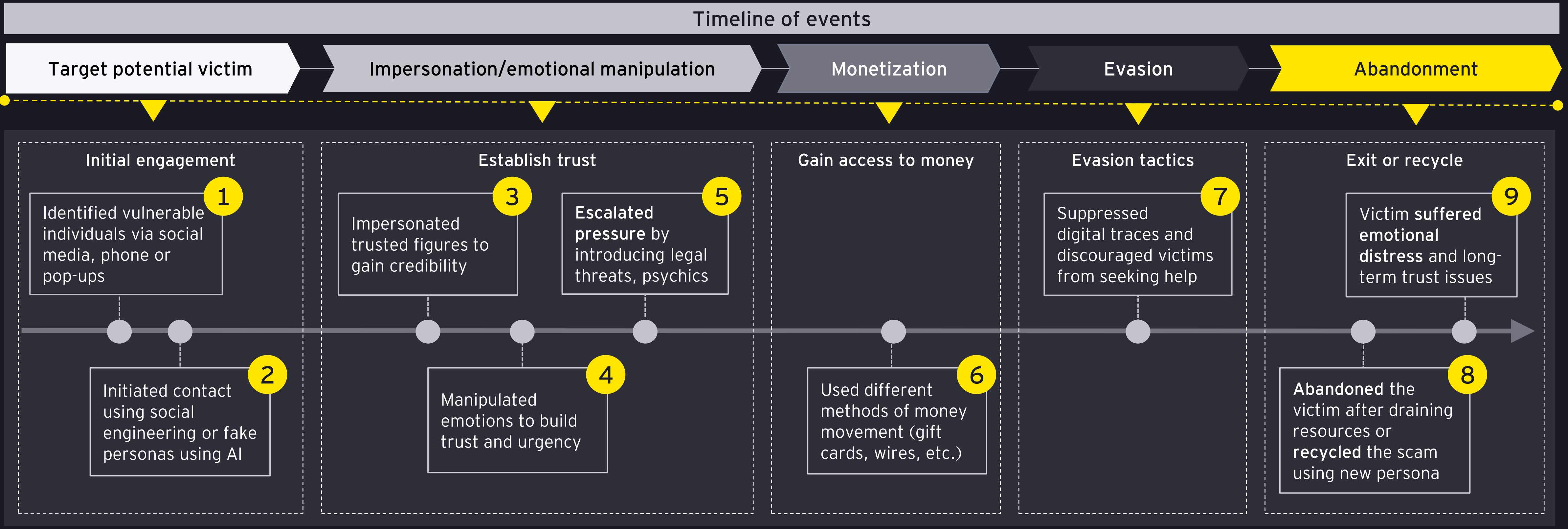
06 **Emotional and authority pressure:**
The scam relied on fear, urgency and impersonated authority to isolate and control the victim's actions over time.

https://www.justice.gov/usao-ct/pr/us-attorneys-office-returns-328573-victim-computer-support-scam
$328,573 returned to elderly Connecticut scam victim | fox61.com

Summarizing the case studies: EFE timeline and scammer patterns

What this tells us about elder financial exploitation (EFE)

Despite different forms – romance and tech support scams – both cases follow a clear **fraud lifecycle**, highlighting the growing threat of EFE and how scams are becoming more digital, emotional and personalized.



Timeline of events

Target potential victim → Impersonation/emotional manipulation → Monetization → Evasion → Abandonment

Initial engagement

1. Identified vulnerable individuals via social media, phone or pop-ups
2. Initiated contact using social engineering or fake personas using AI

Establish trust

3. Impersonated trusted figures to gain credibility
4. Manipulated emotions to build trust and urgency
5. **Escalated pressure** by introducing legal threats, psychics

Gain access to money

6. Used different methods of money movement (gift cards, wires, etc.)

Evasion tactics

7. Suppressed digital traces and discouraged victims from seeking help

Exit or recycle

8. **Abandoned** the victim after draining resources or **recycled** the scam using new persona
9. Victim **suffered emotional distress** and long-term trust issues

EFE : The evolving threat to older adults

Older adults are increasingly targeted for financial scams and abuse – making elder financial exploitation a **growing and urgent concern**.

Latest trends

72 % of elder financial abuse is perpetrated by **people that the victim knows,** which is estimated at approximately **$20.3 billion in total losses.**[1]

90 % Abusers are **family members or trusted individuals** such as caregivers, friends or neighbors in nearly **9 out of 10** elder financial abuse cases.[2]

60+ Older adults (60+) reported a **median loss of $650**, rising to $1,450 for those aged 80+, compared to **$450 for younger adults (18-59)**. [3]

Common EFE fraud typologies

- Advance fee scams
- Tech support scams
- Romance scams
- Friends and family scams
- Government imposter scams

Why are elders at risk?

- Cognitive decline (dementia, confusion)
- Social isolation
- Dependency on others for financial help
- Lack of tech literacy
- High trust in others and perceived authority

How are customers and FIs impacted?

- **Victims:** often don't report, leading to ~$3b in annual losses
- **FIs:** face asset losses, reputational damage, legal repercussions, regulatory scrutiny and higher operational costs
- **Customers:** suffer financial harm, emotional distress and loss of trust in institutions

1. https://www.aarp.org/pri/topics/work-finances-retirement/fraud-consumer-protection/scope-elder-financial-exploitation.html
2. https://www.napsa-now.org/additional-resources-for-financial-exploitation/
3. https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf

Limitations of traditional EFE solutions: a call for AI-driven strategies

Conventional methods to counter elder abuse, such as manual monitoring and reporting, rule-based systems, dependence on customer complaints and generic detection methods, often fall short, lacking scalability and sensitivity to subtle signs of abuse, especially in complex financial contexts ...

Reactive rather than proactive:
Conventional solutions focus on responding to occurred elder abuse rather than preventing it

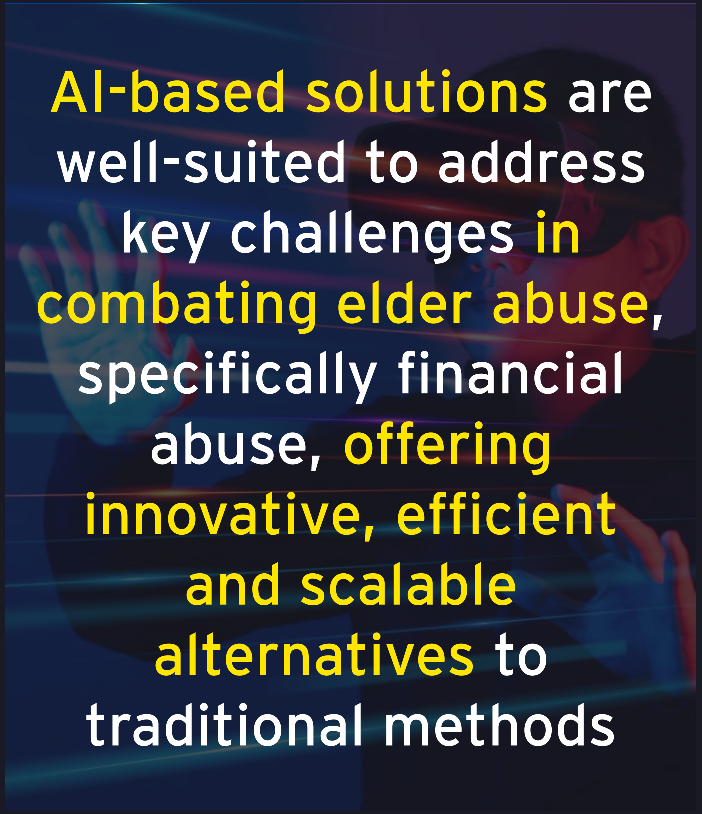
Limited scope of detection:
Limited indicators with manual monitoring and reporting may overlook subtle signs of abuse

Difficulty in analyzing complex data:
Elder exploitation involves sophisticated schemes that require in-depth analysis of behavioral and transactional patterns

Adaptation to new forms of abuse:
As abusers adapt their schemes, conventional methods struggle to keep up with evolving forms of abuse

Scalability:
Conventional human-centric approaches are resource-intensive and may not scale effectively

Crime networks adapt quickly, requiring technologies that can detect evolving schemes impacting elder population



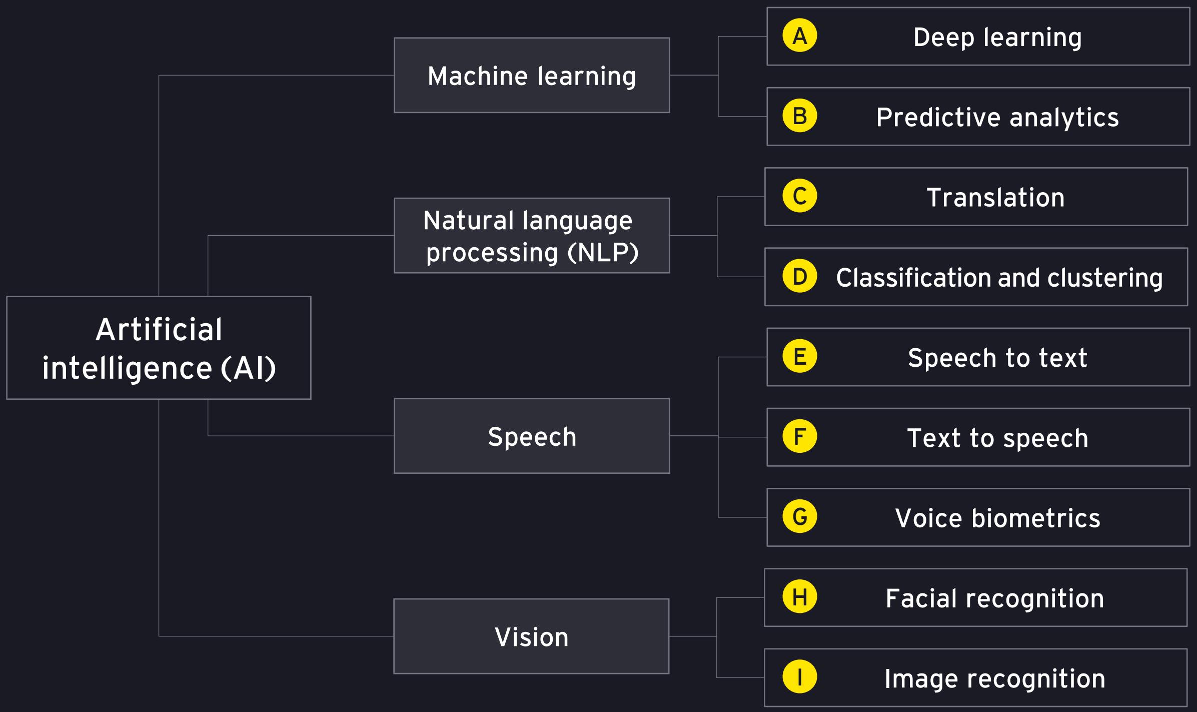
AI-based solutions are well-suited to address key challenges in combating elder abuse, specifically financial abuse, offering innovative, efficient and scalable alternatives to traditional methods

Leveraging next-gen analytics and emerging technologies in fraud

Prioritizing use cases for AI solutions, based on the current state with necessary ethical and compliance considerations, is essential

Example AI capabilities for fraud operations

As augmenting technology fuels, the dynamic world of financial crimes, FIs are pushed to build a comprehensive view to take proactive measures to mitigate existing and new elder abuse scenarios powered by Gen AI/AI capabilities.



Artificial intelligence (AI)

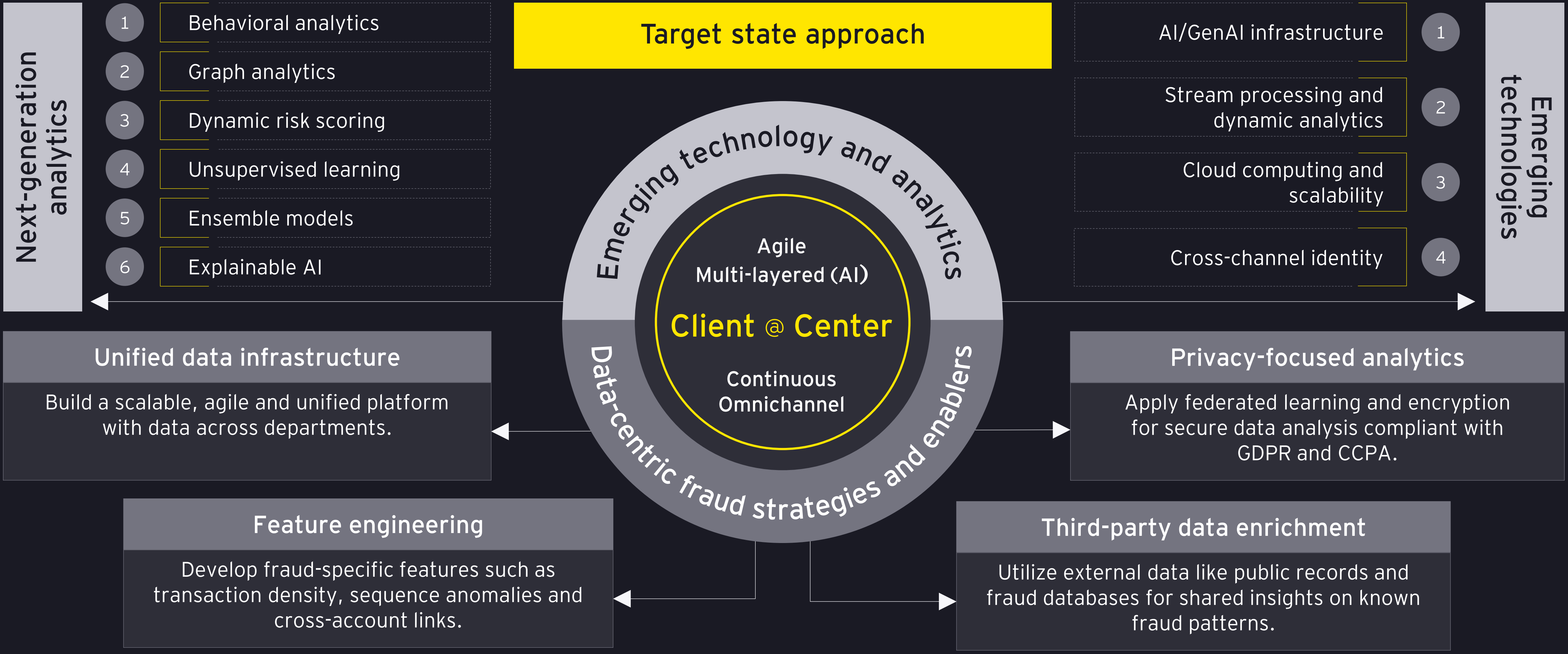
- Machine learning
  - A Deep learning
  - B Predictive analytics
- Natural language processing (NLP)
  - C Translation
  - D Classification and clustering
- Speech
  - E Speech to text
  - F Text to speech
  - G Voice biometrics
- Vision
  - H Facial recognition
  - I Image recognition

Example use cases

Call interaction analytics	Behavioral analytics
Analyze phone conversations and chats (with consent) for signs of coercion or elder abuse	**Analyze elder customers and account activities in real time to identify unusual patterns of potential elder abuse**
Risk predictive analytics	**Payments anomaly detection**
Preemptively identify elders who may be exposed to higher risk of financial abuse	Detects payments that may potentially impact elder population from recurring or hidden charges
Scams detection	**Transactional relationship analytics**
Scan social media platforms to analyze and alert elder account holders related to potential scams and schemes	Detect financial activities as unusual gift from elder customers to new contacts indicative of manipulation

Combating EFE with AI: a new era demands a new ensemble approach

Technology modernization to leverage next-gen analytics driven by data-centric strategies



Target state approach

Next-generation analytics

1. Behavioral analytics
2. Graph analytics
3. Dynamic risk scoring
4. Unsupervised learning
5. Ensemble models
6. Explainable AI

Emerging technologies

1. AI/GenAI infrastructure
2. Stream processing and dynamic analytics
3. Cloud computing and scalability
4. Cross-channel identity

Emerging technology and analytics

Agile

Multi-layered (AI)

Client @ Center

Continuous

Omnichannel

Data-centric fraud strategies and enablers

Unified data infrastructure

Build a scalable, agile and unified platform with data across departments.

Privacy-focused analytics

Apply federated learning and encryption for secure data analysis compliant with GDPR and CCPA.

Feature engineering

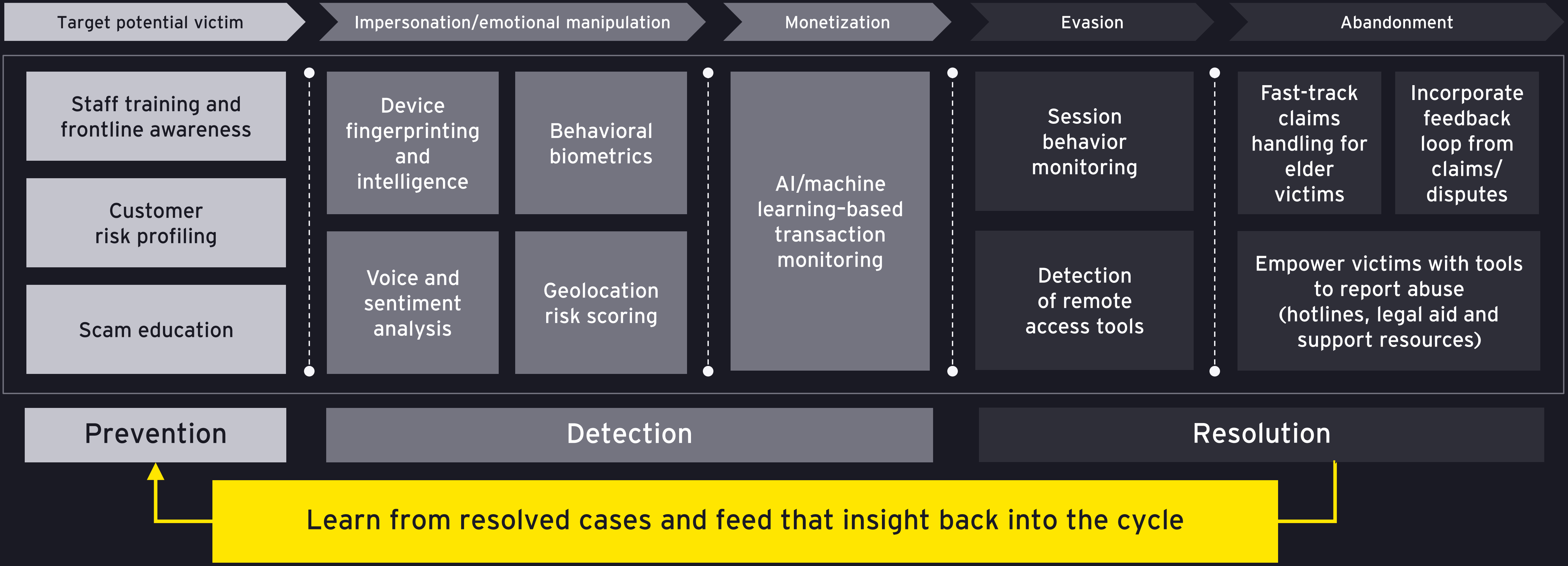
Develop fraud-specific features such as transaction density, sequence anomalies and cross-account links.

Third-party data enrichment

Utilize external data like public records and fraud databases for shared insights on known fraud patterns.

Case studies reimagined: from awareness to response

Revisiting the case studies to highlight **controls** that could have helped institutions to better **prevent, detect and respond** to elder financial exploitation. Continuous learning from resolved cases is critical to combat evolving EFE attack vectors.



Target potential victim

- Staff training and frontline awareness
- Customer risk profiling
- Scam education

Impersonation/emotional manipulation

- Device fingerprinting and intelligence
- Behavioral biometrics
- Voice and sentiment analysis
- Geolocation risk scoring

Monetization

- AI/machine learning-based transaction monitoring

Evasion

- Session behavior monitoring
- Detection of remote access tools

Abandonment

- Fast-track claims handling for elder victims
- Incorporate feedback loop from claims/disputes
- Empower victims with tools to report abuse (hotlines, legal aid and support resources)

Prevention

Detection

Resolution

Learn from resolved cases and feed that insight back into the cycle

Conclusion

EFE causes emotional, financial and psychological harm, often with lasting consequences for victims. As threats escalate, institutions can take the lead, leveraging **AI to strengthen controls from awareness to remediation**, to protect the elderly customers.

1

Institutions can take the lead

Institutions can take the lead to act proactively – building AI-driven frameworks to protect vulnerable clients and stay ahead of scammers

2

AI as an enabler, not a replacement

By leveraging AI-driven insights, institutions can not only detect exploitation, but also prevent fraud, respond swiftly and rebuild trust where it matters most

3

Controls should span the full fraud lifecycle

Institutions should consider embedding controls across all stages – awareness, prevention, detection and remediation – to build a strong fraud risk mitigation program

Q/A

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.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

2504-11372-CS

US SCORE no. 26822-251US

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com