



**THE CAPCO INSTITUTE**  
**JOURNAL**  
OF FINANCIAL TRANSFORMATION

**GOVERNANCE OF CORPORATES**

---

From pattern recognition to decision-making frameworks: Mental models as a game-changer for preventing fraud

LAMIA IRFAN

**BALANCING**  
**INNOVATION & CONTROL**

---

a **wipro** company

**#59** JUNE 2024

# THE CAPCO INSTITUTE

## JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

### Editor

**Shahin Shojai**, Global Head, Capco Institute

### Advisory Board

**Lance Levy**, Strategic Advisor

**Owen Jelf**, Partner, Capco

**Suzanne Muir**, Partner, Capco

**David Oxenstierna**, Partner, Capco

### Editorial Board

**Franklin Allen**, Professor of Finance and Economics and Executive Director of the Brevan Howard Centre, Imperial College London and Professor Emeritus of Finance and Economics, the Wharton School, University of Pennsylvania

**Philippe d'Arvisenet**, Advisor and former Group Chief Economist, BNP Paribas

**Rudi Bogni**, former Chief Executive Officer, UBS Private Banking

**Bruno Bonati**, Former Chairman of the Non-Executive Board, Zuger Kantonalbank, and President, Landis & Gyr Foundation

**Dan Breznitz**, Munk Chair of Innovation Studies, University of Toronto

**Urs Birchler**, Professor Emeritus of Banking, University of Zurich

**Elena Carletti**, Professor of Finance and Dean for Research, Bocconi University, Non-Executive Director, UniCredit S.p.A.

**Lara Cathcart**, Associate Professor of Finance, Imperial College Business School

**Géry Daeninck**, former CEO, Robeco

**Jean Dermine**, Professor of Banking and Finance, INSEAD

**Douglas W. Diamond**, Merton H. Miller Distinguished Service Professor of Finance, University of Chicago

**Elroy Dimson**, Emeritus Professor of Finance, London Business School

**Nicholas Economides**, Professor of Economics, New York University

**Michael Enthoven**, Chairman, NL Financial Investments

**José Luis Escrivá**, President, The Independent Authority for Fiscal Responsibility (AIReF), Spain

**George Feiger**, Pro-Vice-Chancellor and Executive Dean, Aston Business School

**Gregorio de Felice**, Head of Research and Chief Economist, Intesa Sanpaolo

**Maribel Fernandez**, Professor of Computer Science, King's College London

**Allen Ferrell**, Greenfield Professor of Securities Law, Harvard Law School

**Peter Gomber**, Full Professor, Chair of e-Finance, Goethe University Frankfurt

**Wilfried Hauck**, Managing Director, Statera Financial Management GmbH

**Pierre Hillion**, The de Picciotto Professor of Alternative Investments, INSEAD

**Andrei A. Kirilenko**, Reader in Finance, Cambridge Judge Business School, University of Cambridge

**Katja Langenbacher**, Professor of Banking and Corporate Law, House of Finance, Goethe University Frankfurt

**Mitchel Lenson**, Former Group Chief Information Officer, Deutsche Bank

**David T. Llewellyn**, Professor Emeritus of Money and Banking, Loughborough University

**Eva Lomnicka**, Professor of Law, Dickson Poon School of Law, King's College London

**Donald A. Marchand**, Professor Emeritus of Strategy and Information Management, IMD

**Colin Mayer**, Peter Moores Professor of Management Studies, Oxford University

**Francesca Medda**, Professor of Applied Economics and Finance, and Director of UCL Institute of Finance & Technology, University College London

**Pierpaolo Montana**, Group Chief Risk Officer, Mediobanca

**John Taysom**, Visiting Professor of Computer Science, UCL

**D. Sykes Wilford**, W. Frank Hipp Distinguished Chair in Business, The Citadel

# CONTENTS

## GOVERNANCE OF TECHNOLOGY

---

- 08 Data and AI governance**  
**Sarah Gadd**, Chief Data Officer, Bank Julius Baer
- 20 “Data entrepreneurs of the world, unite!” How business leaders should react to the emergence of data cooperatives**  
**José Parra-Moyano**, Professor of Digital Strategy, IMD
- 26 Revolutionizing data governance for AI large language models**  
**Xavier Labrecque St-Vincent**, Associate Partner, Capco  
**Varenya Prasad**, Principal Consultant, Capco
- 32 Municipal data engines: Community privacy and homeland security**  
**Nick Reese**, Cofounder and COO, Frontier Foundry Corporation
- 40 Human/AI augmentation: The need to develop a new people-centric function to fully benefit from AI**  
**Maurizio Marcon**, Strategy Lead, Analytics and AI Products, Group Data and Intelligence, UniCredit
- 50 Building FinTech and innovation ecosystems**  
**Ross P. Buckley**, Australian Research Council Laureate Fellow and Scientia Professor, Faculty of Law and Justice, UNSW Sydney  
**Douglas W. Arner**, Kerry Holdings Professor in Law and Associate Director, HKU-Standard Chartered FinTech Academy, University of Hong Kong  
**Dirk A. Zetzsche**, ADA Chair in Financial Law, University of Luxembourg  
**Lucien J. van Romburg**, Postdoctoral Research Fellow, UNSW Sydney
- 56 Use and misuse of interpretability in machine learning**  
**Brian Clark**, Rensselaer Polytechnic Institute  
**Majeed Simaan**, Stevens Institute of Technology  
**Akhtar Siddique**, Office of the Comptroller of the Currency
- 60 Implementing data governance: Insights and strategies from the higher education sector**  
**Patrick Cernea**, Director, Data Strategy and Governance, York University, Canada  
**Margaret Kierylo**, Assistant Vice-President, Institutional Planning and Chief Data Officer, York University, Canada
- 70 AI, business, and international human rights**  
**Mark Chinen**, Professor, Seattle University School of Law

## GOVERNANCE OF SUSTAINABILITY

---

### 82 Government incentives accelerating the shift to green energy

**Ben Meng**, Chairman, Asia Pacific, Franklin Templeton

**Anne Simpson**, Global Head of Sustainability, Franklin Templeton

### 92 Governance of sustainable finance

**Adam William Chalmers**, Senior Lecturer (Associate Professor) in Politics and International Relations, University of Edinburgh

**Robyn Klingler-Vidra**, Reader (Associate Professor) in Entrepreneurship and Sustainability, King's Business School

**David Aikman**, Professor of Finance and Director of the Qatar Centre for Global Banking and Finance, King's Business School

**Karlygash Kuralbayeva**, Senior Lecturer in Economics, School of Social Science and Public Policy, King's College London

**Timothy Foreman**, Research Scholar, International Institute for Applied Systems Analysis (IIASA)

### 102 The role of institutional investors in ESG: Diverging trends in U.S. and European corporate governance landscapes

**Anne LaFarre**, Associate Professor in Corporate Law and Corporate Governance, Tilburg Law School

### 112 How banks respond to climate transition risk

**Brunella Bruno**, Tenured Researcher, Finance Department and Baffi, Bocconi University

### 118 How financial sector leadership shapes sustainable finance as a transformative opportunity: The case of the Swiss Stewardship Code

**Aurélia Fäh**, Senior Sustainability Expert, Asset Management Association Switzerland (AMAS)

## GOVERNANCE OF CORPORATES

---

### 126 Cycles in private equity markets

**Michel Degosciu**, CEO, LPX AG

**Karl Schmedders**, Professor of Finance, IMD

**Maximilian Werner**, Associate Director and Research Fellow, IMD

### 134 Higher capital requirements on banks: Are they worth it?

**Josef Schroth**, Research Advisor, Financial Stability Department, Bank of Canada

### 140 From pattern recognition to decision-making frameworks: Mental models as a game-changer for preventing fraud

**Lamia Irfan**, Applied Research Lead, Innovation Design Labs, Capco

### 148 Global financial order at a crossroads: Do CBDCs lead to Balkanization or harmonization?

**Cheng-Yun (CY) Tsang**, Associate Professor and Executive Group Member (Industry Partnership), Centre for Commercial Law and Regulatory Studies (CLARS), Monash University Faculty of Law (Monash Law)

**Ping-Kuei Chen**, Associate Professor, Department of Diplomacy, National Chengchi University

### 158 Artificial intelligence in financial services

**Charles Kerrigan**, Partner, CMS

**Antonia Bain**, Lawyer, CMS



**DEAR READER,**

In my new role as CEO of Capco, I am very pleased to welcome you to the latest edition of the Capco Journal, titled **Balancing Innovation and Control**.

The financial services and energy sectors are poised for another transformative year. At Capco, we recognize that this is a new era where innovation, expertise, adaptability, and speed of execution will be valued as never before.

Success will be determined based on exceptional strategic thinking, and the ability to leverage innovative new technology, including GenAI, while balancing a laser focus on risk and resilience. Leaders across the financial services and energy industries recognize the transformative benefits of strong governance while needing to find the optimal balance between innovation and control.

This edition of the Capco Journal thus examines the critical role of balancing innovation and control in technology, with a particular focus on data, AI, and sustainability, with wider corporate governance considerations. As always, our authors include leading academics, senior financial services executives, and Capco's own subject matter experts.

I hope that you will find the articles in this edition truly thought provoking, and that our contributors' insights prove valuable, as you consider your institution's future approach to managing innovation in a controlled environment.

My thanks and appreciation to our contributors and our readers.



Annie Rowland, **Capco CEO**

# FROM PATTERN RECOGNITION TO DECISION-MAKING FRAMEWORKS: MENTAL MODELS AS A GAME-CHANGER FOR PREVENTING FRAUD

LAMIA IRFAN | Applied Research Lead, Innovation Design Labs, Capco

## ABSTRACT

In the ever-evolving fraud prevention landscape, mental models are emerging as a game-changer. By serving as cognitive frameworks that guide our understanding and interpretation of fraudulent activities, mental models enable financial institutions to elevate their fraud prevention efforts. This article explores the role of mental models in preventing fraud, from pattern recognition to decision-making frameworks, highlighting their significance in safeguarding assets and enhancing efficacy.

## 1. INTRODUCTION

The global cost of fraud, encompassing losses, prevention measures, and staffing expenses, has been estimated to be around U.S.\$5.4 trillion [Cox (2023)]. This poses a substantial hurdle for financial institutions, given that they must navigate regulatory mandates, ethical dilemmas related to artificial intelligence (AI), and intricate legacy systems. To combat fraud effectively, understanding the underlying mechanisms and motivations driving fraudulent activities is essential. In recent years, mental models have gained traction as powerful tools for enhancing fraud prevention strategies. By leveraging cognitive frameworks, financial institutions can gain deeper insights into fraud patterns, enabling proactive detection and mitigation.

## 2. DEFINITION OF FRAUD

In its simplest form, fraud involves a falsehood and a financial gain. Financial fraud encompasses a wide range of deceptive practices aimed at gaining an unfair advantage or financial benefit. According to Reurink (2018), financial fraud involves

the deliberate or reckless dissemination of false, incomplete, or manipulative information related to financial goods, services, or investment opportunities, violating legal stipulations.

### 2.1 Understanding the complex world of fraud

The insurance industry in the U.K. serves as a microcosm of the challenges posed by fraud, with significant financial implications. The insurance industry has long grappled with the daunting issue of fraud, a problem underscored by recent statistics. In 2022, the industry incurred £1.1 billion (approximately U.S.\$1.4 billion) in costs, mirroring figures from 2021 and 2020 [ABI (2022)]. Yet, there is a noteworthy decline of 19% in the number of detected fraud cases. Adding to the complexity, the average value per fraud has surged by 20% to £15,000, emphasizing the evolving nature of this challenge.

To compound the issue, fraud represents over 40% of all reported crimes in England and Wales [NCA (2023)]. However, underreporting remains a concern, with just 43% of fraud victims reporting their cases. Perceptions of triviality, concerns

about privacy, or independent resolution attempts, deter many from reporting. The consequences of insurance fraud ripple across the industry, escalating costs for insurers, leading to higher policyholder premiums, eroding trust, and posing a threat to the industry's stability.

Even though U.K. organizations invest an average of £600,000 (approximately U.S.\$ 750,000) annually in cybersecurity for fraud prevention, the problem persists.

## 2.2 Types of fraud

Fraud can take various forms, including hard fraud and soft fraud. Hard fraud involves premeditated schemes aimed at claiming payments for covered losses, often orchestrated by organized crime syndicates. Soft fraud, on the other hand, entails opportunistic behaviors such as exaggerating legitimate claims for personal gain. Frauds encompass a range of deceptive practices, including false financial disclosures, financial scams, and financial mis-selling.

- **False financial disclosures**, entailing deceptive statements about entities' financial status, sow an illusion of transparency while exacerbating information asymmetry [Black (2006)]. In the insurance industry, the prevalence of fraud, particularly arising from false disclosures during applications and claims, has intensified amidst the ongoing cost of living crisis. Between March 2022 and April 2023, opportunistic fraud cases surged by 61%, with motor insurance fraud comprising 51% of these cases and property insurance fraud 29%. The repercussions are severe, leading to higher premiums, policy voidances, claim delays or denials, increased financial burdens for honest policyholders, and legal consequences such as

criminal charges, fines, and reputational damage.

- **In financial scams**, fraudsters deceive individuals into voluntarily participating and handing over funds or sensitive information. They rely on lies and fabricated facts, inducing victims to make decisions based on false promises or threats [Pressman (1998)].
- **Fraudulent financial mis-selling** refers to manipulative marketing or selling of financial products, knowing that they are unsuitable for the consumer's needs. Unlike financial scams, mis-selling practices involve suggestive communication that creates misleading impressions [Pressman (1998)].

## 2.3 The fraud triangle

The fraud triangle, conceptualized by Donald Cressey in the 1950s, provides valuable insights into the psychological and situational factors driving fraudulent behavior. At its core, the fraud triangle consists of three key elements: opportunity, pressure, and rationalization (Figure 1). These elements offer a framework for understanding how individuals justify and engage in fraudulent activities.

Rationalization, one of the components of the fraud triangle, is particularly relevant to mental models. It involves the cognitive processes through which individuals justify or excuse their fraudulent behavior, often by minimizing its moral or ethical implications. Fraudsters employ various rationalizations to justify their actions, portraying themselves as victims of circumstances or viewing their behavior as necessary given perceived unfairness or inadequacy. This aspect of the fraud triangle highlights the role of cognitive frameworks or mental models in shaping individuals' perceptions and decisions.

Figure 1: The fraud triangle



Source: Cressey (1953)

Similarly, the pressure component of the fraud triangle underscores the impact of external or internal forces that compel individuals to commit fraud. These pressures may include financial difficulties, personal crises, or unrealistic performance expectations. Mental models, which guide individuals' understanding and interpretation of the world around them, can influence how they perceive and respond to these pressures, potentially leading them to rationalize fraudulent behavior as a means of coping with or alleviating these pressures.

### 3. EXPLORATION OF MENTAL MODELS IN FRAUD PREVENTION

Mental models serve as cognitive frameworks that help individuals understand and navigate complex situations, playing a crucial role in fraud prevention.

Within the realm of behavioral science, a mental model is a cognitive framework or representation that individuals use to understand the world, make sense of information, and interpret their experiences. It encompasses beliefs, assumptions,

perceptions, and knowledge structures that influence how people perceive, analyze, and respond to situations. Mental models help individuals organize information, predict outcomes, and make decisions by providing a simplified and structured representation of complex phenomena or systems. To gain a comprehensive understanding of the mental models at play in fraud, it is essential to consider it at the micro, meso, and macro levels (Figure 2).

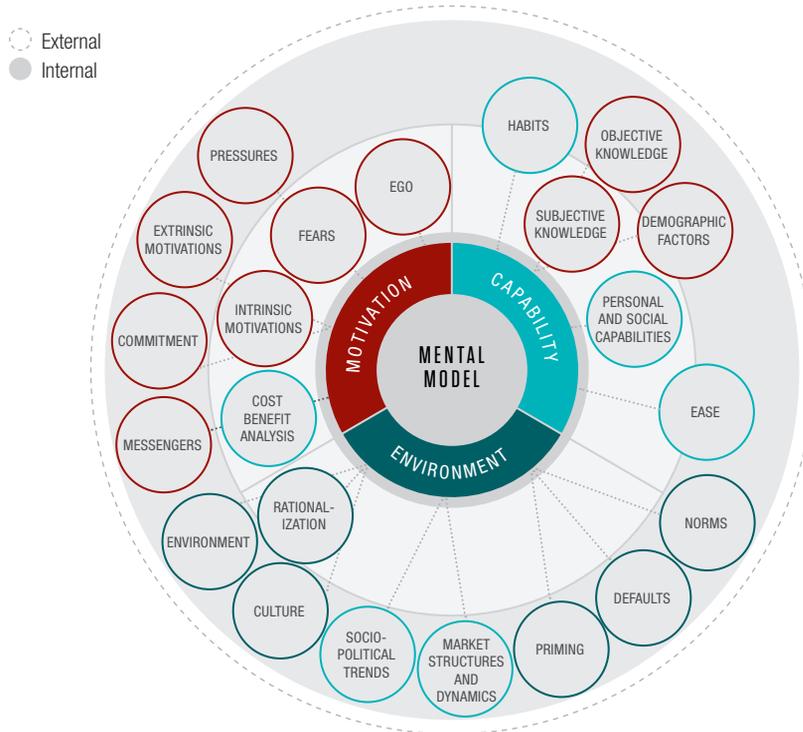
#### 3.1 Internal factors: The micro perspective

Understanding fraud at a micro level entails analyzing demographic profiles, personality types, motivations, internal pressures, and rationalizations.

##### 3.1.1 DEMOGRAPHIC PROFILE OF FRAUDSTERS

This involves scrutinizing age, gender, and ethnicity to gain insights into those involved in white-collar crimes. Typically, white-collar criminals are individuals over 40, predominantly male, and of white ethnicity. They often hold positions such as company owners or officers, with socio-economic standings significantly above the national average [Gekoski et al. (2022)].

Figure 2: Mental model framework



Our mental model framework looks at internal and external drivers that influence the ways in which we think and act. It outlines the complexities and interconnections between different drivers that, when understood and addressed, support development of human-centric product designs.

### 3.1.2 PERSONALITY CHARACTERISTICS

Fraudsters exhibit distinct traits such as overconfidence, cultural hedonism, narcissistic personality disorder, and a lack of self-control. Their behavior is often driven by a strong business mindset prioritizing competence and success, motivated by personal gain and the desire to outperform competitors. They often rationalize their actions, focusing on short-term benefits without considering larger ethical ramifications.

### 3.1.3 RATIONALIZATIONS

Rationalizations for fraud often include the “Robin Hood” ideology, where perpetrators justify their actions as redistributing wealth from the rich to the needy. Additionally, some individuals perceive fraud as a victimless crime, minimizing the harm inflicted on faceless entities like corporations. However, these rationalizations overlook the moral implications and real-world consequences of fraudulent behavior, perpetuating unethical actions in financial transactions.

### 3.1.4 OCCUPATIONAL POSITIONS

Exploring the professional roles held by fraudsters, including company owners or officers, and their socio-economic status, provides further insights into their behaviors.

### 3.1.5 MOTIVATIONS FOR FRAUD

Fraudsters’ motivations often exceed mere greed, as they harbor intrinsic desires for recognition and respect alongside financial gain. They may perceive their schemes as legitimate ventures akin to entrepreneurial pursuits [Frankel (2012)], fostering an illusion of trustworthiness crucial for successful investment scams [Stolowy et al. (2014)]. This mindset may also lead operators to overlook unsustainable elements within their schemes [Naylor (2007)].

### 3.1.6 PSYCHOLOGICAL PRESSURES

Internal pressures, such as the fear of failure and potential loss of status, are key drivers pushing individuals toward fraudulent activities. Motivations for white-collar fraudsters are complex, often fueled by a combination of factors including greed, a desire for social likability, and pressure to maintain an image of success.

## 3.2 External factors: The meso and macro perspective

Examining fraud from a meso and macro perspective involves analyzing affinity networks, opportunities for fraud, perceived risk and reward, control mechanisms, and socio-political and economic influences.

### 3.2.1 AFFINITY NETWORKS

Analysis of social, business, or personal networks used by fraudsters to identify co-conspirators and victims, fostering a sense of trust and familiarity [Stolowy et al. (2014)].

### 3.2.2 OPPORTUNITIES FOR FRAUD

Identification of factors such as unmonitored access to resources and unsuspecting victims that create opportunities for fraudulent activities. Access to vulnerable victims is facilitated through various means, such as “lead lists” or “mooch lists” readily available online for a nominal fee [Baker and Faulkner (2003), Nash et al. (2013)].

### 3.2.3 PERCEIVED RISK AND REWARD

Understanding how fraudsters perceive fraud schemes as “low-risk and high-return activities”, influencing their decision to engage in fraudulent acts.

### 3.2.4 CONTROL MECHANISMS

Examination of the role of law enforcement agencies, regulatory bodies, auditors, and cybersecurity experts in detecting and combating fraud. Inadequate oversight, including failures by external auditors and regulatory authorities, can enable scams to thrive [Geis (2013), Shapiro (2013), Markopolos (2010)].

### 3.2.5 SOCIO-POLITICAL AND ECONOMIC INFLUENCES

Analysis of socio-political trends, such as the cost-of-living crisis, housing shortages, and market dynamics, reveals potential drivers behind individuals resorting to fraud as a means of coping with financial challenges or gaining a competitive edge. Moreover, societal norms emphasizing success over ethical acquisition may incentivize individuals to prioritize financial gain regardless of the means [Trahan et al. (2005), Young (2013)]. Fraudsters adeptly exploit financial market opacity, particularly in hedge funds, leveraging technological advancements like the Internet to maintain anonymity [Frankel (2012), Blois (2013), Shapiro (2013), Stolowy et al. (2014)].

### 3.3 Fraudster personas

Mental models play a crucial role in shaping personas of fraudsters. Three prevalent archetypes are presented: the opportunistic fraudster, the con artist, and the trusted insider.

#### 3.3.1 THE OPPORTUNISTIC FRAUDSTER

Opportunistic fraudsters are often seemingly law-abiding citizens. Their offenses typically involve spur-of-the-moment decisions, lacking deliberate attempts to target insurers. Instead, they stem from chance occurrences and the pressing need or desire for money. Such opportunities arise during legitimate claims processes, when introduced by others, when the fraud is relatively straightforward, or when the fraudster is emotionally unstable. The primary driver for these individuals is financial gain, often overshadowing their consideration of risk factors. Moreover, fraud is seen as an easily committed and justifiable crime, with a low risk of detection and limited police interest.

#### 3.3.2 THE CON ARTIST

Despite their charming facade, con artists frequently demonstrate a lack of empathy, often deflecting responsibility onto their victims [Lewis (2012), Frankel (2012)]. Motivated by grandiose visions of success, they perceive their fraudulent ventures as legitimate businesses, effectively gaining the trust of unsuspecting investors [Frankel (2012), Stolowy et al. (2014)]. Scammers employ various deceptive tactics, such as exploiting trusted brand names, while preying on victims' emotional vulnerabilities, particularly greed and the desire for quick financial gains, often creating a false sense of urgency in their schemes. Genuine financial scams follow a structured approach, targeting individuals with high disposable incomes or financial vulnerabilities through promises of high returns or threats of financial consequences if they do not comply. Additionally, in romance scams, con artists utilize tactics such as mirroring, where they mimic their victims' personalities, preferences, and emotions to establish a false sense of intimacy and trust, ultimately exploiting their emotional vulnerabilities for financial gain.

#### 3.3.3 THE TRUSTED INSIDER

Internal fraudsters often fit a profile of middle-aged white males in stable white-collar positions, as owners or officers in their companies, enjoying above-average socio-economic status [Gekoski et al. (2022)]. The link between age and white-collar crime lies in opportunity, as it takes time to

attain positions conducive to large-scale offenses. A common trait shared among offenders, regardless of their status, is salesmanship – the ability to earn trust and manipulate others, essential for both legitimate success and fraudulent activities.

Two paths diverge among offenders: one group climbs the corporate ladder through hard work and salesmanship but finds ethical compromises necessary for continued advancement, while the other achieves success but faces financial pressures that lead to fraudulent behavior to maintain their lifestyle. This latter group may feel genuine remorse for their actions once exposed, driven not by ego but fear of failure.

## 4. USING SITUATIONAL CRIME PREVENTION TO COMBAT FRAUD

Situational crime prevention is an approach to crime prevention that focuses on manipulating the immediate environment in which crimes occur to reduce opportunities for criminal behavior and increase the perceived risks and difficulties for potential offenders [Freilich and Newman (2017)]. This approach recognizes that crime is often opportunistic and influenced by environmental factors, such as the design of physical spaces, the presence of security measures, and the routines of potential targets (Figure 3).

Figure 3: Situational crime prevention



Situational crime prevention focuses on addressing the immediate situational factors that contribute to fraudulent activities, aiming to create environments that are less conducive to fraud and more challenging for fraudsters to exploit.

Key principles of situational crime prevention involve manipulating the immediate environment to deter criminal behavior. These tactics include:

- **Increase effort:** implementing measures that make committing fraud more difficult by adding obstacles or increasing the effort required. This could involve enhancing security measures such as multi-factor authentication, encryption protocols, or identity verification processes to create barriers and deter fraudulent activities.
- **Increase risk:** enhancing the perceived risk of engaging in fraudulent behavior by increasing the likelihood of detection, apprehension, or punishment. This might include deploying advanced fraud detection algorithms, conducting regular audits and reviews, or collaborating with law enforcement agencies to investigate and prosecute offenders, thereby making fraudsters feel more exposed and vulnerable to consequences.
- **Reduce reward:** decreasing the potential benefits or gains of engaging in fraudulent activities to make it less appealing. Strategies might include implementing stringent financial controls, conducting thorough background checks on employees and vendors, or enhancing customer verification processes to mitigate the incentives for fraudulent transactions or schemes.
- **Reduce provocations:** minimizing factors that might provoke or incentivize fraudulent behavior. This could involve implementing fraud awareness and training programs for employees and customers, enhancing internal controls and oversight mechanisms, or improving communication channels to address grievances and concerns effectively, thereby reducing the likelihood of individuals resorting to fraud as a response to perceived injustices or pressures.

By applying these principles, situational crime prevention aims to modify the immediate context in which crimes occur, making criminal behavior less attractive or feasible while promoting safer and more secure environments for individuals and communities.

Overall, situational crime prevention emphasizes proactive measures to modify the immediate environment in ways that discourage criminal behavior and promote community safety. To counteract these cognitive biases and rationalizations, situational crime prevention strategies leverage mental models to disrupt the perceived benefits of fraud and increase the perceived risks and difficulties for potential offenders.

This may involve implementing controls and safeguards within financial systems and processes to increase the effort required to commit fraud, enhancing surveillance and monitoring to increase the risks of detection, and promoting a culture of accountability and integrity to remove excuses for criminal behavior.

Furthermore, situational crime prevention in the context of fraud utilizes mental models to inform the design of intervention strategies that target specific situational factors associated with fraudulent activities. By understanding the cognitive processes and decision-making patterns of fraudsters, organizations can develop tailored prevention measures that address the underlying motivations and environmental cues that contribute to fraud.

In essence, situational crime prevention for fraud recognizes the interplay between cognitive factors, environmental conditions, and criminal behavior, and seeks to manipulate the situational context to deter fraud and promote ethical conduct. By leveraging mental models to understand the cognitive processes underlying fraud, organizations can implement targeted interventions that effectively disrupt the mechanisms driving fraudulent activities and safeguard against financial losses.

## 5. UTILIZING MENTAL MODELS WITHIN FINANCIAL SERVICES

Mental models facilitate pattern recognition, anomaly detection, decision making, behavioral analysis, and collaboration among financial institutions and law enforcement agencies.

- **Pattern recognition and anomaly detection:** mental models play a crucial role in financial crime prevention, particularly in pattern recognition and anomaly detection. By employing advanced algorithms and machine learning techniques, institutions can analyze financial data in real-time to identify suspicious patterns and deviations from normal behavior. This enables proactive measures to be taken to prevent fraudulent activities before they escalate.
- **Decision-making frameworks:** mental models provide decision-making frameworks that guide fraud investigators and analysts in taking appropriate action. These frameworks consider various factors, including the severity of the fraud, the likelihood of false positives, and the impact on legitimate customers. By incorporating risk-based decision-making principles, financial institutions can prioritize their resources effectively and respond to fraud incidents promptly.

- **Behavioral analysis and psychometric profiling:** in addition, mental models excel in behavioral analysis and psychometric profiling, aiding in the identification of potential perpetrators as well as vulnerable victims. By analyzing behavioral patterns and personality traits of fraudsters and victims alike, institutions can tailor their detection methods to effectively mitigate specific threats.
- **Service design:** in service design, mental models can enhance the creation of customer journeys. This involves integrating prompts and pauses to stimulate ethical reflection among customers as they navigate through the journey. By encouraging individuals to pause and contemplate the broader consequences of their actions, they can develop a deeper awareness of the ethical implications inherent in their decisions. This approach fosters a more responsible and socially conscious customer experience. Service staff can also undergo training to identify victim vulnerabilities and tactics employed by fraudsters.
- **Collaborative intelligence and information sharing:** mental models facilitate collaborative intelligence and information sharing among financial institutions and law enforcement agencies. By sharing data and insights, organizations can collectively identify emerging fraud trends, share best practices, and coordinate their efforts to combat fraud more effectively. This collaborative approach enables institutions to leverage the collective expertise and resources of the entire ecosystem, leading to more robust fraud prevention measures.
- **Continuous learning and adaptation:** finally, mental models enable continuous learning and adaptation in response to evolving fraud threats. By analyzing past incidents and identifying areas for improvement, financial institutions can refine their fraud prevention strategies and stay ahead of emerging threats. This iterative process of learning and adaptation is essential for maintaining the effectiveness of fraud prevention measures in a rapidly changing environment.

## 6. CONCLUSION

Most organizations have traditionally focused their fraud strategies on detection and prevention measures, often relying on technological solutions and procedural controls. However, by incorporating mental models into their approach, organizations can gain deeper insights into the motivations, behaviors, and psychological factors driving both fraudsters and victims. Understanding the cognitive biases, decision-making processes, and situational factors that influence individuals involved in fraudulent activities can help organizations develop more effective strategies for detecting, mitigating, and responding to fraud. By adopting a behavioral science perspective and leveraging mental models, organizations can enhance their fraud strategies by addressing root causes, designing targeted interventions, and fostering a culture of vigilance and resilience.

## REFERENCES

- ABI, 2022, "Fraud," Association of British Insurers, <https://tinyurl.com/2bc959z7>
- Baker, W. E., and R. R. Faulkner, 2003, "Diffusion of fraud: intermediate economic crime and investor dynamics," *Criminology* 41:4, 1173–1206
- Black, W. K., 2006, "Book review: control fraud theory v. the protocols," *Crime, Law and Social Change* 45:3, 241–258
- Blois, K., 2013, "Affinity fraud and trust within financial markets," *Journal of Financial Crime* 20:2, 186–202
- Cornish, D. B., and R. V. Clarke, 2003, "Opportunities, precipitators and criminal decisions: a reply to Wortley's critique of situational crime prevention," in Smith, M. J., and D. B. Cornish (eds.), *Theory for practice in situational crime prevention, crime prevention studies*, Vol. 16, Criminal Justice Press
- Cox, M., 2023, "Fraud predictions 2024: scams, siloes and upstream polluters," Fico blog, <https://tinyurl.com/47a82nww>
- Cressey, D., 1953, *Other people's money: a study in the social psychology of embezzlement*, Free Press
- Frankel, T., 2012, *The Ponzi scheme puzzle: a history and analysis of con artists and victims*, Oxford University Press
- Freilich, J., and G. Newman, 2017, "Situational crime prevention," *Oxford Research Encyclopaedia of Criminology*, March 29, <https://tinyurl.com/2kkh85ab>
- Geis, G., 2013, "Unaccountable external auditors and their role in the economic meltdown," in Will, S., S. Handelman, and D. C. Brotherton (eds.), *How they got away with it: white collar criminals and the financial meltdown*, Columbia University Press
- Gekoski, A., J. R. Adler, and T. McSweeney, 2022, "Profiling the fraudster: findings from a rapid evidence assessment," *Global Crime* 23:4, 422–442
- IFED, 2023, "Police warn of rise in bogus insurance claims as people turn to fraud amid cost of living pressures," The City of London Police's Insurance Fraud Enforcement Department (IFED), <https://tinyurl.com/4mp4wtkv>
- Lewis, M. K., 2012, "New dogs, old tricks. why do Ponzi schemes succeed?" *Accounting Forum* 36:4, 294–309
- Markopolos, H., 2010, *No one would listen: a true financial thriller*, John Wiley & Sons
- Nash, R., M. Bouchard, and A. Malm, 2013, "Investing in people: the role of social networks in the diffusion of a large-scale fraud," *Social Networks* 35:4, 686–698
- NCA, 2023, *Fraud*, National Crime Agency, <https://tinyurl.com/jmu78m2f>
- Naylor, R. Thomas, 2007, "The Alchemy of Fraud: Investment Scams in the Precious-metals Mining Business," in: *Crime, Law and Social Change* 47, 89–120
- Pressman, S., 1998, "On financial frauds and their causes," *American Journal of Economics and Sociology* 57:4, 405–421
- Reurink, A., 2018, "Financial fraud: a literature review," *Journal of Economic Surveys* 32:5, 1292–1325
- Shapiro, D., 2013, "Generating alpha return: how Ponzi schemes lure the unwary in an unregulated market," in Will, S., S. Handelman, and D. C. Brotherton (eds.), *How they got away with it: white collar criminals and the financial meltdown*, Columbia University Press
- Stolowy, H., M. Messner, T. Jeanjean, and C. R. Baker, 2014, "The construction of a trustworthy investment opportunity: insights from the madoff fraud," *Contemporary Accounting Research* 31:2, 354–397
- Trahan, A., J. W. Marquart, and J. Mullings, 2005, "Fraud and the American dream: toward an understanding of fraud victimisation," *Deviant Behaviour* 26:6, 601–620
- Young, J., 2013, "Bernie Madoff, finance capital, and the anomic society," in Will, S., S. Handelman, and D. C. Brotherton (eds.), *How they got away with it: white collar criminals and the financial meltdown*, Columbia University Press

© 2024 The Capital Markets Company (UK) Limited. All rights reserved.

This document was produced for information purposes only and is for the exclusive use of the recipient.

This publication has been prepared for general guidance purposes, and is indicative and subject to change. It does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (whether express or implied) is given as to the accuracy or completeness of the information contained in this publication and The Capital Markets Company BVBA and its affiliated companies globally (collectively "Capco") does not, to the extent permissible by law, assume any liability or duty of care for any consequences of the acts or omissions of those relying on information contained in this publication, or for any decision taken based upon it.

## ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy focused in the financial services industry. Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit [www.capco.com](http://www.capco.com) or follow us on Facebook, YouTube, LinkedIn and Instagram.

## WORLDWIDE OFFICES

### APAC

Bengaluru – Electronic City  
Bengaluru – Sarjapur Road  
Bangkok  
Chennai  
Gurugram  
Hong Kong  
Hyderabad  
Kuala Lumpur  
Mumbai  
Pune  
Singapore

### MIDDLE EAST

Dubai

### EUROPE

Berlin  
Bratislava  
Brussels  
Dusseldorf  
Edinburgh  
Frankfurt  
Geneva  
Glasgow  
London  
Milan  
Paris  
Vienna  
Warsaw  
Zurich

### NORTH AMERICA

Charlotte  
Chicago  
Dallas  
Hartford  
Houston  
New York  
Orlando  
Toronto

### SOUTH AMERICA

São Paulo

[WWW.CAPCO.COM](http://WWW.CAPCO.COM)



# CAPCO

a wipro company