Deloitte.

Innovation in Counter Fraud Analytics

In the Middle East since 1926

May 2024

Financial Fraud is growing, with fraudsters leveraging information stolen through data breaches and social engineering schemes targeting those with limited controls or preventive measures. Fraud schemes have also grown in complexity and sophistication. Bad actors are leveraging improvements in technology to commit fraud at scale through automation, obscuring their identities through VPNs, obfuscated IP addresses, and anonymous browsers. Additionally, through the dark web, bad actors can sell and distribute fraud schemes through fraud playbooks. To help effectively combat these growing risks, Deloitte brings a cutting-edge analytical based approach and data science techniques that can be tailored to each client's needs and circumstances.

Deloitte can help organizations integrate these methodologies and techniques into their current program by utilizing diverse business and technology skillsets and deep industry expertise.

Global Fraud Threats

As fraud is constantly evolving and growing, it has become one of the main challenges that financial institutions are facing nowadays

Economic value and financial loss
In 2023, scammers stole over **$1 trillion** from victims, according to the Global Anti-Scam Alliance.

Increased Operational costs
25% of companies in US and UK lost over **$1M** to fraud in 2023

Opportunities & Solutions
70% of organizations expect to increase spending on AI or machine learning in the next 1-2 years.

Top 10 global external fraud trends

Potential impact in Middle East

- Online identity theft for mule accounts creation
- Increase in e-commerce non 3DS as a mean of monetizing payments
- SIM swapping to obtain OTPs to authorize transactions
- Low awareness of suspicious Emails or APPs
- Xpays as an alternative to the card-not-present (CNP)

- Business Email Compromise
- Impersonation of financial institutions employees to trick customers into executing monetary transactions
- RAT to access the bank's digital channels from the victim's own device
- Cryptocurrency or investment scams as an alternative of monetization
- ATMs and points-of-sale as a source of stolen information

Increased sophistication of fraud techniques
Automation, artificial intelligence, machine learning, and other advanced tools allow fraudulent activities to take place with greater precision and accuracy

Emergence of new fraud channel
Growing popularity of digital payment methods and cryptocurrencies has introduced new avenues for fraudulent activities.

Data Breaches and Information Threat
Increasing interconnectedness of systems and the storage of vast amounts of sensitive data have made organizations more vulnerable.

The information described is based on a **market research** and on the experience of **Deloitte** with financial institutions; information collected from different geographies as Europe, UK, Americas and Middle East

Global Best Practices in Counter Fraud Analytics
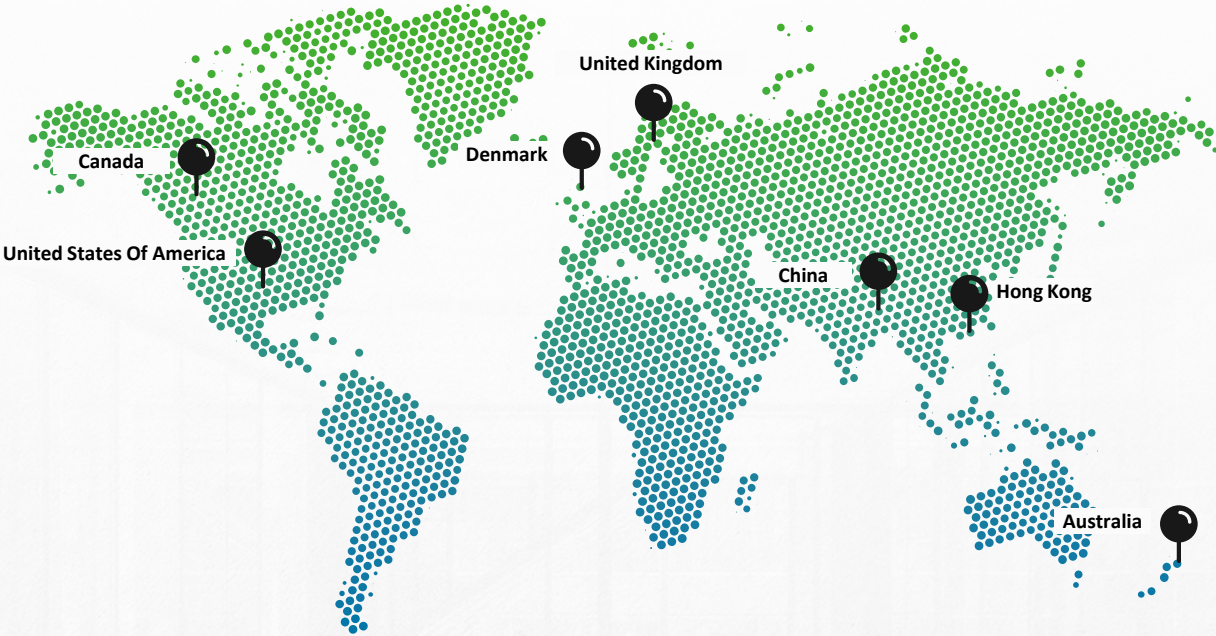
United States Of America
J.P. Morgan, USA uses AI to enhance payment efficiency and reduce fraud by automating payment validation screening and providing insights like cash flow analysis to clients as needed, thereby reducing fraud and improving customer experience

Canada
Canadian Credit Union implemented a real-time transaction-level monitoring and alerting system, that provided end-to-end visibility of debit card transactions, and quickly identified performance issues within their network , ensuring reliable and secure transaction processing.

Denmark
Danske Bank leverages AI and Deep Learning to significantly reduce false positives and increase true positives in fraud detection, enhancing their overall fraud management capabilities.

China
is leveraging a combination of big data analytics, AI systems, facial recognition technology, application monitoring, and GIS tracking as tools for preventing fraud.

Hong Kong
Vast databases are being developed containing extremely detailed information on individuals and organizations. Information technology has provided new opportunities for data collection and management, facilitating demographic segmentation (data mining) and new and more extensive forms of management information analysis.

Australia
ANZ, through its Bluenotes platform, utilizes machine learning and AI to enhance fraud prevention mechanisms. These technologies help in analyzing vast amounts of transaction data in real-time, enabling the detection of patterns and anomalies that may indicate fraudulent activities. Machine learning models are trained to recognize typical customer behavior, and any deviation from these patterns can trigger alerts for further investigation. Additionally, AI is used to improve the accuracy and efficiency of real-time monitoring systems, ensuring that legitimate transactions are processed smoothly while potentially fraudulent ones are flagged and reviewed.

United Kingdom
Clearspeed, a UK based company, provides a unique voice analytics service that assesses risk through user responses to automated questions. Users receive a digital link, listen to, and answer two to four questions. The solution analyzes these responses in near real-time and generates risk signals that inform the organization of potential risks. This risk triage solution enables a bank to fast-track "green" cases while focusing its limited resources on the cases genuinely presenting a higher risk

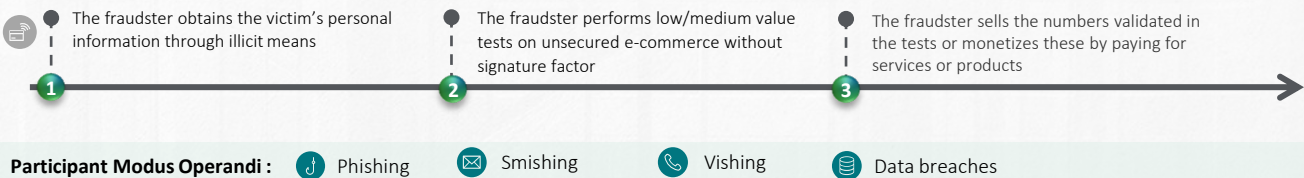# External fraud threats that most affect financial institutions

Online identity theft for mule accounts creation

In this type of threat, the fraudster obtains the victim's personal information through illicit means with the intention of impersonating the legal person to create new accounts in financial institutions that will be used as mule accounts for receiving illicit funds.

1. The fraudster obtains the victim's personal information through illicit means
2. The fraudster impersonates the victim to create a new account in the financial institution
3. The fraudster uses the mule account to move the fraudulent funds or to sell accounts

Participant Modus Operandi : Phishing · Social engineering · Malware · Data breaches
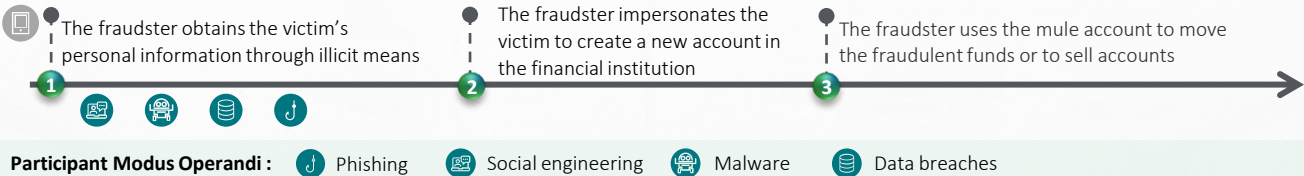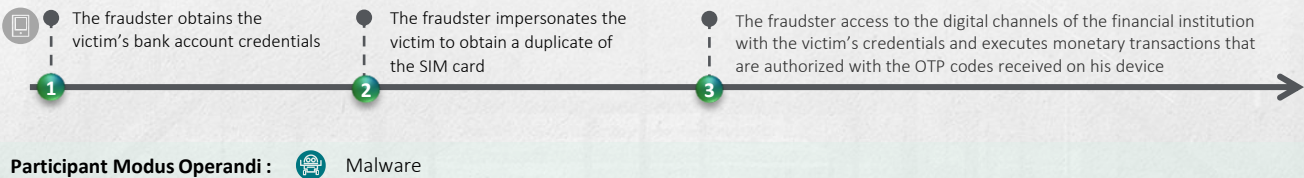
Increase in e-commerce non 3DS as a means of monetizing payments

E-commerce that do not have 3DS are used by fraudsters to monetize/validate the credentials of the cards obtained. Once the credentials are validated, the fraudster proceeds to sell this information in the deep web.

1. The fraudster obtains the victim's personal information through illicit means
2. The fraudster performs low/medium value tests on unsecured e-commerce without signature factor
3. The fraudster sells the numbers validated in the tests or monetizes these by paying for services or products

Participant Modus Operandi : Phishing · Smishing · Vishing · Data breaches
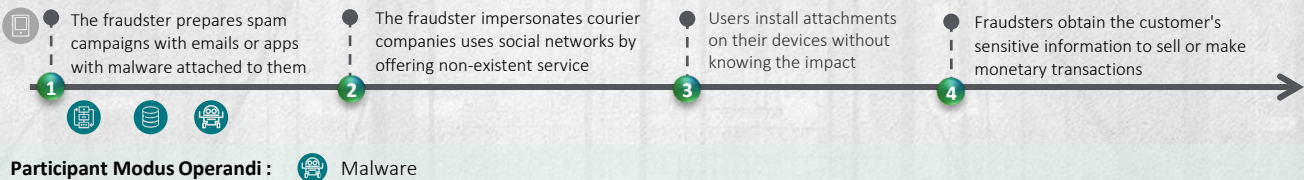
SIM swapping to obtain OTPs to authorize transactions

In a SIM Swap, the fraudster impersonates the victim to trick a cellular service provider to obtain a duplicate of the SIM card of the victim. With the bank account credentials previously obtained, the fraudster is able to execute and authorize payments (via OTP) from his device.

1. The fraudster obtains the victim's bank account credentials
2. The fraudster impersonates the victim to obtain a duplicate of the SIM card
3. The fraudster access to the digital channels of the financial institution with the victim's credentials and executes monetary transactions that are authorized with the OTP codes received on his device

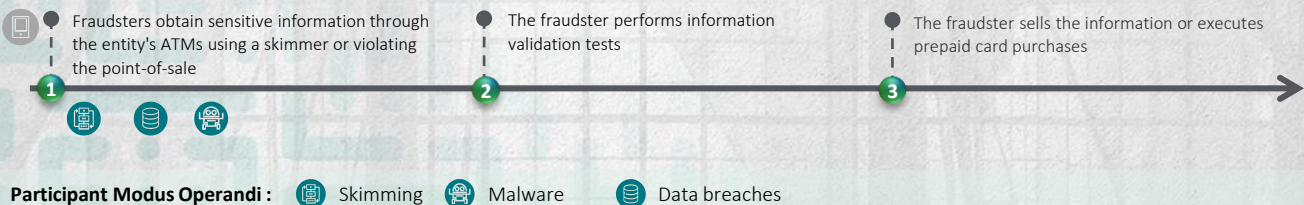**Participant Modus Operandi :** Malware

Low awareness of suspicious Emails or APPs

The lack of knowledge of people with downloading any attachment or application on their devices is quite recurrent and the fraudster is also aware of it. The main factor is absolute permission control on devices is allowed.

1. The fraudster prepares spam campaigns with emails or apps with malware attached to them
2. The fraudster impersonates courier companies uses social networks by offering non-existent service
3. Users install attachments on their devices without knowing the impact
4. Fraudsters obtain the customer's sensitive information to sell or make monetary transactions

Participant Modus Operandi : Malware

ATMs and points-of-sale as a source of stolen information

In this type of threat, the fraudster obtains the victim's personal information through illicit means with the intention of impersonating the legal person to create new accounts in financial institutions that will be used as mule accounts for receiving illicit funds.
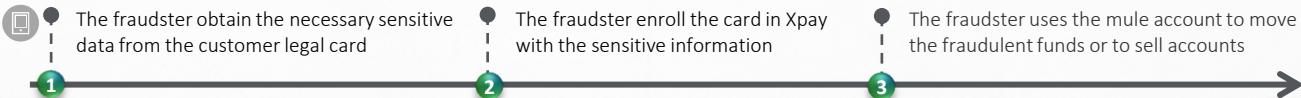
1. Fraudsters obtain sensitive information through the entity's ATMs using a skimmer or violating the point-of-sale
2. The fraudster performs information validation tests
3. The fraudster sells the information or executes prepaid card purchases

Participant Modus Operandi : Skimming · Malware · Data breaches

External fraud threats that most affect financial institutions

Xpays as an alternative to the card-not-present (CNP)

The ease and convenience offered by this type of service presents a great opportunity for the fraudster. Once the fraudster has obtained the sensitive data of the victim's card, it is easy for them to complete the Xpay enrolment and execute purchases in stores.
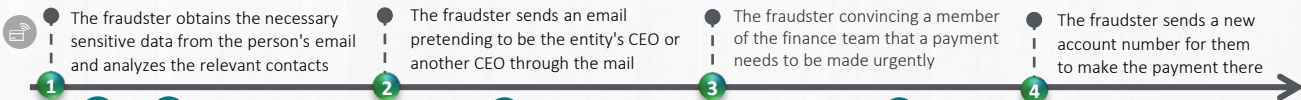
1 The fraudster obtain the necessary sensitive data from the customer legal card

2 The fraudster enroll the card in Xpay with the sensitive information

3 The fraudster uses the mule account to move the fraudulent funds or to sell accounts

Participant Modus Operandi: Phishing | Smishing | Social engineering | Vishing | Data breaches

Business Email Compromise

This fraud type, currently on the rise, even though having a low probability of occurring, have a high impact, due to the high amounts defrauded. Fraudsters pose as a trusted person from a well-known company to make payments to other account numbers that they do not have registered.
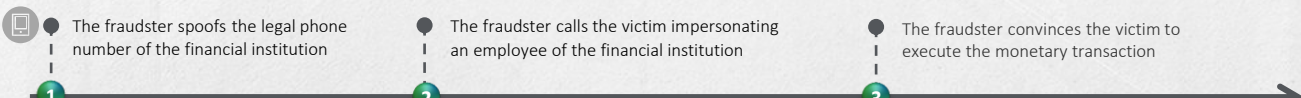
1 The fraudster obtains the necessary sensitive data from the person's email and analyzes the relevant contacts

2 The fraudster sends an email pretending to be the entity's CEO or another CEO through the mail

3 The fraudster convincing a member of the finance team that a payment needs to be made urgently

4 The fraudster sends a new account number for them to make the payment there

Participant Modus Operandi: Phishing | Social engineering | Data breaches

Impersonation of financial institutions employees to trick customers into executing monetary transactions

Scammers pretend to be a trusted person from the financial institution so that the customer can carry out operations or make them think that to release a blocked service they must give authorization.
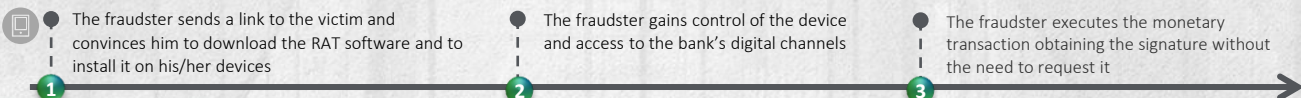
1 The fraudster spoofs the legal phone number of the financial institution

2 The fraudster calls the victim impersonating an employee of the financial institution

3 The fraudster convinces the victim to execute the monetary transaction

Participant Modus Operandi: Spoofing | Social engineering

RAT to access the bank's digital channels from the victim's own device

The possibility of being able to use remote environments is serving the fraudster as a very important means of executing fraud given the difficulty of being detected "impersonating" the client's legal equipment.
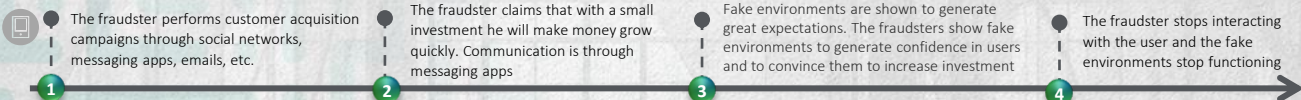
1 The fraudster sends a link to the victim and convinces him to download the RAT software and to install it on his/her devices

2 The fraudster gains control of the device and access to the bank's digital channels

3 The fraudster executes the monetary transaction obtaining the signature without the need to request it

Participant Modus Operandi: Malware | Social engineering

Cryptocurrency or investment scams as an alternative of monetization

Currently, scams are being one of the main concerns globally. The scammers use different methods to gain trust of the customers and convince them to execute the fraudulent transaction.

1 The fraudster performs customer acquisition campaigns through social networks, messaging apps, emails, etc.

2 The fraudster claims that with a small investment he will make money grow quickly. Communication is through messaging apps

3 Fake environments are shown to generate great expectations. The fraudsters show fake environments to generate confidence in users and to convince them to increase investment

4 The fraudster stops interacting with the user and the fake environments stop functioning

Participant Modus Operandi: Skimming | Malware | Data breaches

Unlocking value with fraud analytics:

Fraud analytics can significantly enhance the value delivered by the banking sector. By leveraging advanced analytics and data insights, banks can not only mitigate the risk of fraudulent transactions but also enhance operational efficiency, comply with regulatory standards, and improve customer trust.

Loss reduction associated with fraudulent transaction through Real-time prevention and improved detection accuracy

Fine reduction and reputational gain through Government standard compliance

Cost reduction through automation, freeing up resources that can be redirected to other value-adding activities and help standardize responses to fraud alerts, reducing human error.

Value creation for customer; prevent customer churn through fraud incidents and attract new customers for exemplary performance

Improve fraud prevention and detection rules and scenarios through insights gained from fraud analytics on fraud patterns and behaviors, anticipating potential future threats.

Transition from reactive to proactive fraud detection by leveraging machine learning models and scoring systems to develop both financial and non-financial behavioral scores.

Key Challenges in Banking Sector

The banking sector in Middle East faces obstacles in preventing and detecting fraud. Addressing these challenges is crucial for enhancing the effectiveness of fraud management systems.

- Length of time to process fraud alerts.
- High Level of False Positives

- Lack of an exhaustive set of rules implemented in the if-then logic rule-based models.

- Overreliance on Manual Processes that could be automated.
- Machine learning, Deep Learning and Artificial Intelligence are not leveraged to enhance performance

- Relying on a reactive rather than a proactive approach to prevent and detect fraud

- A shortage of trained data analyst, data scientist is hindering the development of effective anti-fraud solutions.
- Team operating in Silos which can prevent a unified view necessary for detecting complex fraud schemes.

Counter Fraud Framework : Analytics applied

By utilizing comprehensive predictive models, tailored risk assessments, and data visualization, banks can establish strong governance, accurately identify fraudulent activities, and take timely, proportionate actions. This proactive approach to managing fraud risks enhances overall security and ensures compliance.

Governance Through Analytics:

Providing comprehensive visualizations, dashboards, detailed reports, and analytics tools to give decision-makers a clearer understanding of the fraud landscape to establish insight driven governance and controls.

Detection with Precision:

Deploying predictive models and machine learning techniques to proactively recognize risky patterns and detect fraud, while utilizing both Financial and non-Financial historical Behavioral data.

Counter Fraud Framework

Prevention enhanced by Analytics:

Comprehensive list of rules and controls specifically tailored to the bank's unique fraud landscape. Rules are defined by analyzing historical data and employing a robust fraud risk assessment framework.

Responsive Actions:

Scoring and prioritizing risks based on their severity and potential impact. Automating the response enables immediate actions to ensure timely proportionate action.

Deloitte's Program Integrity Framework

Demonstrated solutions, Rapid result

Deloitte has helped banks and financial institutions across the globe to effectively leverage analytics to drive impactful results in preventing and detecting fraud.

Deloitte's Program Integrity Framework
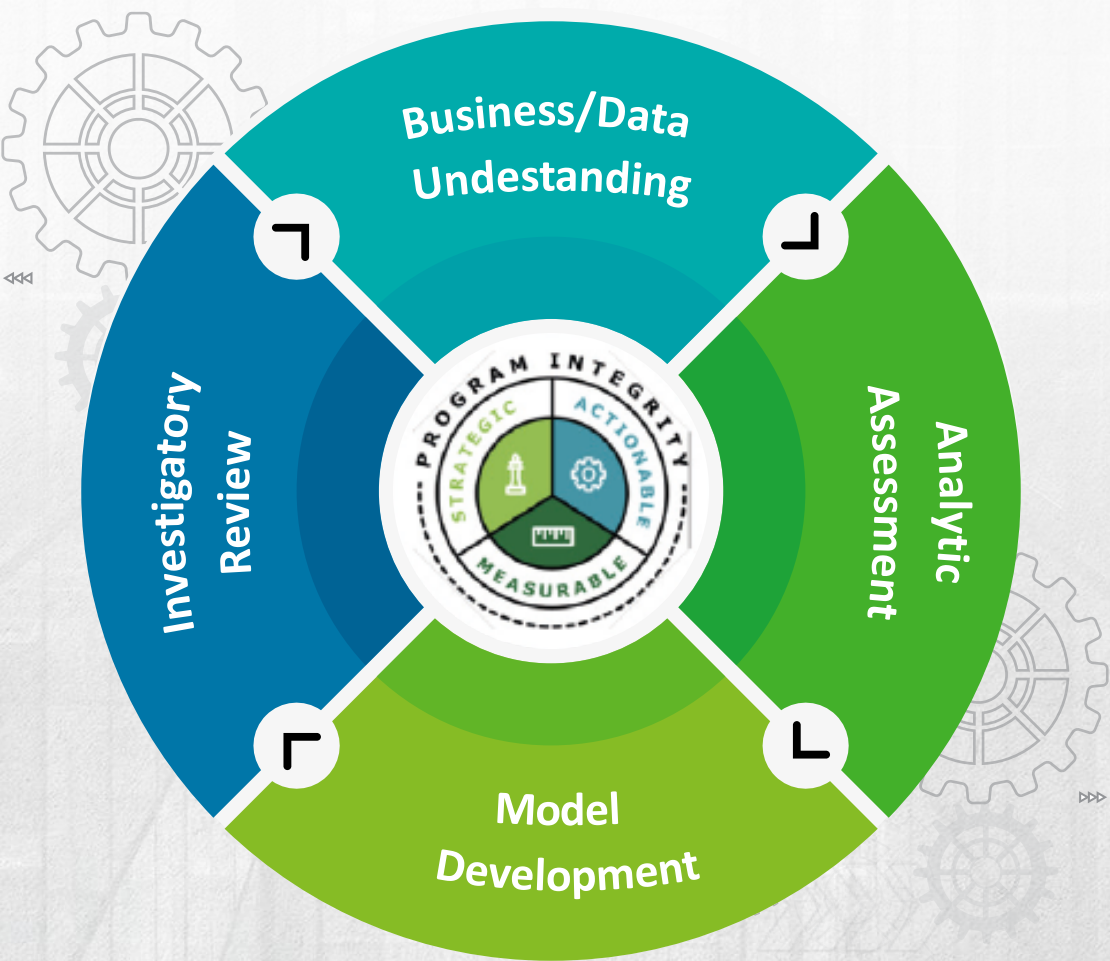
Through this accrued experience, Deloitte has developed and maintains a deep repository of tested techniques. These techniques span the full spectrum of approaches and can be rapidly tailored to fit the unique needs of our clients.

Our experience in combining these techniques to understand, prevent and detect fraud has made us an industry leader and allow us to stay ahead of evolving threats.

Analytics and Modeling Techniques

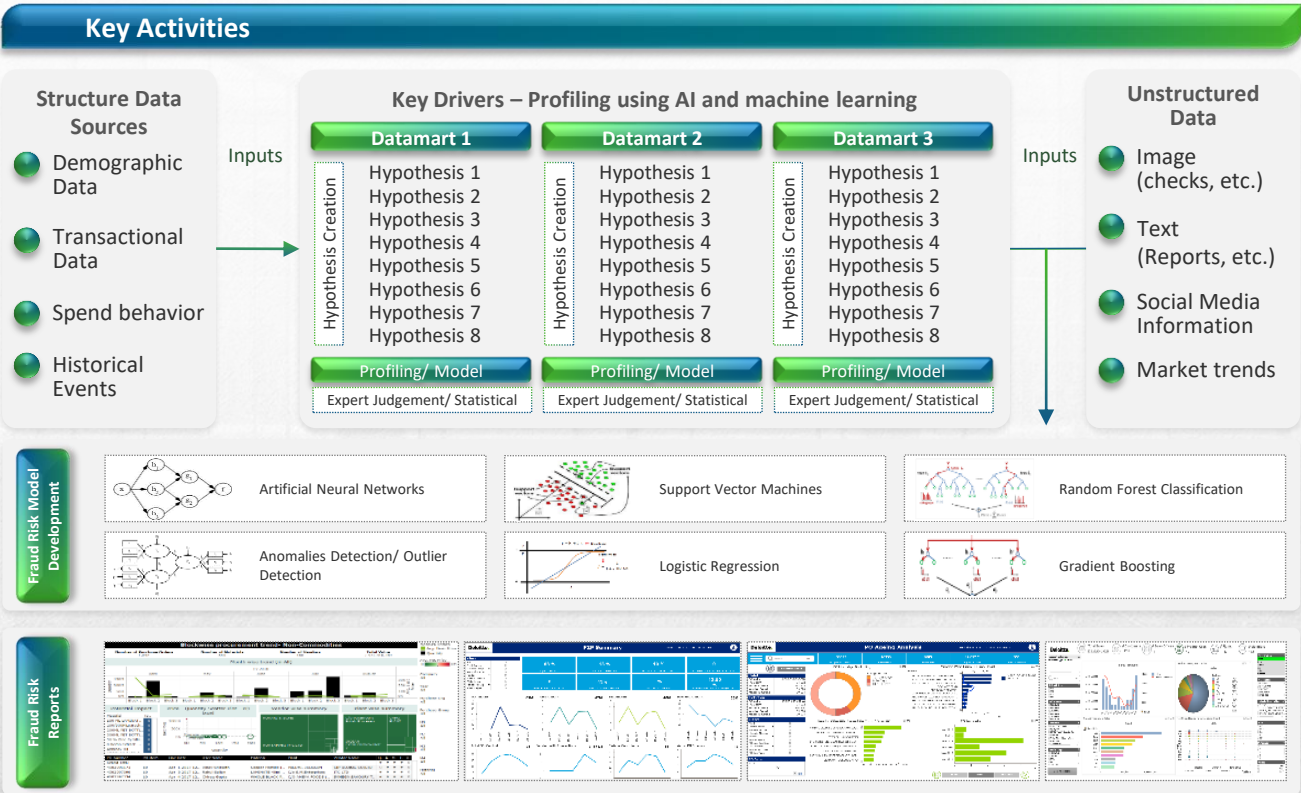These techniques can be grouped into four primary buckets: Rules, Anomaly, Predictive, and Network.

Approach	Description	Examples
Rules	If-then logic based on known high-risk activity and when business rules are susceptible to more complex schemes.	• Sequence detection • Business rules • Bust out
Anomaly	Identifies activity that deviates from observed norms when there is limited existing knowledge of fraud schemes.	• Hierarchical clustering • Isolation forests • Dbscan
Predictive	Machine learning algorithms that identify activity that share defining characteristics with previously identified instances of Fraud.	• Logistic regression • Agent-based models • Neural nets
Network	Provides the ability to identify meaningful connections between data points, enabling the identification of fraud networks.	• Topological modeling • Louvain modularity • PageRank

Through Deloitte's experience in delivering program integrity analytics and modeling services across industries, we can provide strategic insights to select and tailor the complement of techniques to enable protection.

Deloitte's Overarching Framework

A comprehensive end to end solution for rapid fraud detection and reporting

Deloitte has a robust framework for fraud prevention/detection and reporting that leverages advanced analytics and machine learning techniques. With years of experience in the industry, Deloitte provides a comprehensive solution that ensures rapid detection and accurate reporting of fraudulent activities.

Key Activities

Structure Data Sources

- Demographic Data
- Transactional Data
- Spend behavior
- Historical Events

Inputs →

Key Drivers – Profiling using AI and machine learning

Datamart 1	Datamart 2	Datamart 3
Hypothesis 1	Hypothesis 1	Hypothesis 1
Hypothesis 2	Hypothesis 2	Hypothesis 2
Hypothesis 3	Hypothesis 3	Hypothesis 3
Hypothesis 4	Hypothesis 4	Hypothesis 4
Hypothesis 5	Hypothesis 5	Hypothesis 5
Hypothesis 6	Hypothesis 6	Hypothesis 6
Hypothesis 7	Hypothesis 7	Hypothesis 7
Hypothesis 8	Hypothesis 8	Hypothesis 8
Profiling/ Model	Profiling/ Model	Profiling/ Model
Expert Judgement/ Statistical	Expert Judgement/ Statistical	Expert Judgement/ Statistical

(Hypothesis Creation)

← Inputs

Unstructured Data

- Image (checks, etc.)
- Text (Reports, etc.)
- Social Media Information
- Market trends

Fraud Risk Model Development

Artificial Neural Networks	Support Vector Machines
Anomalies Detection/ Outlier Detection	Logistic Regression
Random Forest Classification	Gradient Boosting

Fraud Risk Reports

The goal of any fraud-detection system is to make the most optimal use of the limited available information, or in other words to maximize the fraction of fraudulent cases among the cases that generate alerts without having a detrimental impact on customer satisfaction.

Through this framework, Deloitte enhances the efficiency and accuracy of fraud prevention/detection, significantly reducing the cost associated with fraudulent activities. Our extensive experience in fraud prevention/detection and risk management ensures that our clients receive unparalleled protection against fraud.

Deloitte's Fraud Risk Assessment Process
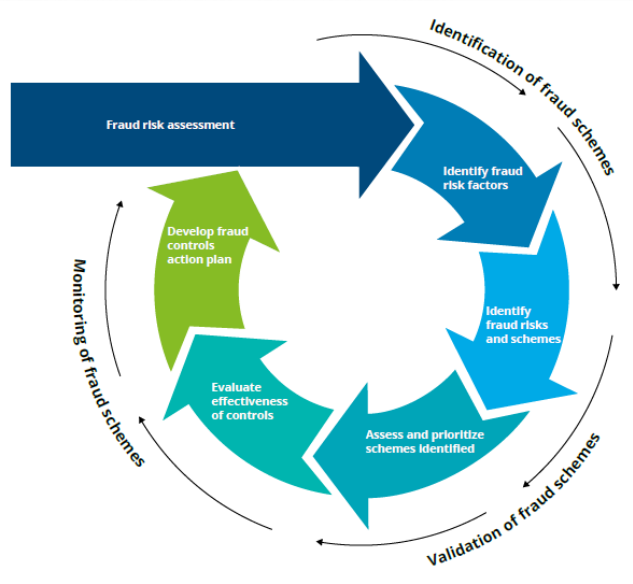
Deloitte's Fraud Risk Assessment (FRA) Process is a scheme and scenario-based risk assessment designed to identify, assess, prioritize, and respond to potential fraud risks facing an organization. The aim is to think about how someone might commit a fraud against the organization and whether the organization has appropriate controls to mitigate the chances of that fraud happening.

Deloitte's Fraud Risk Assessment Process:

1 — **Identify fraud risk factors**	The FRA process begins with identifying fraud risk factors that span operations, geographies, and other dimensions of the business. This step is crucial as it lays the foundation for understanding the various ways in which fraud can manifest within the organization.
2 — **Identify fraud risks and schemes**	Once the risk factors are identified, the next step is to determine the actual fraud risks and the shape the associated fraud schemes might take.
3 — **Assess and prioritize schemes identified**	Prioritization will consider the likelihood, impact or significance, potential for management override, and absence of internal controls to identify the inherent risk for each fraud scheme. Once prioritized, it's important to identify and map existing internal controls to the prioritized fraud schemes, considering both preventive and detective controls.
4 — **Evaluate effectiveness of controls**	The next step involves evaluating the effectiveness of the existing internal and operational controls. This involve control testing to determine if they are operating as intended.
5 — **Develop fraud controls action plan**	Finally, leverage the results of control testing to determine if they're operating effectively. Where they aren't, or where adequate controls are missing, remediate.

Deloitte's Product and services for Counter Fraud Analytics

Illustration of Deloitte Product and services related to Counter Fraud Analytics.

Services

- Provide a comprehensive list of tailored rules and controls designed to effectively prevent and detect fraudulent activities.
- Develop and implement machine learning models, Risk Scoring models and behavioral analytics for enhanced fraud detection and prevention, utilizing both supervised and unsupervised learning techniques.
- Offer services to assess and validate third-party models, ensuring they meet regulatory standards and operational requirements.
- Leverage advanced text analytics to extract and analyze unstructured data for insights into fraud risks and patterns.

Deloitte Platform

- Fraud Data Platform to drive effective development, data-based training, ongoing monitoring, seamless execution and continuous enhancement of Fraud models.
- Centralized analytics platform can provide insights across various departments (Risk, Finance, Operations).
- Data-centric approach to decision-making, emphasizing its role in fostering a culture that prioritizes analytical insights for fraud prevention.

Enhance fraud risk management with better, faster, & data-powered Fraud modeling abilities	
Better capabilities and ecosystem . . .	. . . Fraud scoring/alerting with real-time context available at any consumption point
Faster delivery and innovation . . .	. . . Experimentation in hours and deployment in weeks not months
Empowered organization to innovate . . .	. . . Flexible and accessible data for data scientists and all risk/compliance users

- ▶ Advance fraud management abilities for today and for the future

- ▶ Accelerate and support new fraud risk mitigation initiatives

- ▶ Evolve fraud models faster and innovate with less complexity

- ▶ Minimize fraud losses and increase regulatory compliance

- ▶ Maximize value from your technology and people

- ▶ Achieve Customer 360 view and better serve your customers

Our Differentiators

Our Success Stories
We have assisted multiple banks and financial institutions in fraud model development, validation and have designed and implemented Fraud Risk Management Frameworks in the region and globally.

Our tools & accelerators
At Deloitte we have a library of in-house proprietary tools and accelerators that we leverage to deliver our services effectively and efficiently.

Our commitment
Given our unparalleled expertise and experience, we are committed to support in the entire journey and assist in the successful model risk management for the organization.

Our subject matter expert
We bring access to unequalled expertise and insights through our team who have worked with global and regional Banks, providing globally tried and tested methodologies boosting your time-to-value.

Our operating model
We provide flexible delivery options best suited for your need allowing you to make an informed choice on the operating model: Project Driven Managed Service and Loan Staffing/ Secondment.

Contact

Ravi Ranjan
General Partner
rranjan2@deloitte.com
+966568868836
+971581276610

Kinshuk Pal
Partner
kipal@deloitte.com
+966 542919639

Bikranta Raychaudhuri
Director
braychaudhuri@deloitte.com
+97156363 7727

Deloitte.

About Deloitte

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms and their related entities are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

Deloitte & Touche (M.E.) is a member firm of Deloitte Touche Tohmatsu Limited (DTTL) and is a leading professional services firm established in the Middle East region with uninterrupted presence since 1926. DTME's presence in the Middle East region is established through its affiliated independent legal entities which are licensed to operate and to provide services under the applicable laws and regulations of the relevant country. DTME's affiliates and related entities cannot oblige each other and/or DTME, and when providing services, each affiliate and related entity engages directly and independently with its own clients and shall only be liable only for its own acts or omissions and not those of any other affiliate.

Deloitte provides audit, tax, consulting, financial advisory and risk advisory services through 25 offices in 14 countries with more than 3,300 partners, directors and staff. It is a Tier 1 Tax advisor in the GCC region since 2010 (according to the International Tax Review World Tax Rankings). It has also received numerous awards in the last few years which include best Advisory and Consultancy Firm of the Year 2016 in the CFO Middle East awards, best employer in the Middle East, the Middle East Training & Development Excellence Award by the Institute of Chartered Accountants in England and Wales (ICAEW), as well as the best CSR integrated organization.

Designed By CoRe Creative Services. RITM178450.