LTIMindtree

WHITEPAPER

# Securing the Future

## A Practical Solution to Financial Crimes

LTIMindtree

# Table of Contents

# Executive Summary

Financial crime (FinCrime) covers a spectrum of unlawful activities that exploit financial systems for individual gain. It includes money laundering, fraud, terror financing, cybercrime, bribery, and corruption. These crimes result in losses and compromise the integrity and stability of financial institutions and economies.

Tackling FinCrime is crucial to safeguard the stability of financial systems and shield individuals and businesses from fraud and economic harm. Robust measures ensure compliance with international standards, uphold investor confidence, and protect the reputation of financial institutions. Building trust within the financial sector attracts investments, driving economic growth and stability.

This whitepaper focuses on identifying the tools and technologies available to combat FinCrime, ascertaining the challenges, and proposing a comprehensive and future proof solution. FinSafeX, the customised solution mentioned, provides a systematic approach by collecting, processing, analyzing, and generating reports and dashboards for the consumption of law enforcement agencies. Data is collected from different reporting entities and loaded into the system after being processed through extraction and transformation. This information is then cleansed through data refinement and enrichment, after which, the system performs risk scoring for suspected entities. Finally, reports and insights are generated. The solution also provides loosely coupled systems that work independently and collaborate with each other for output generation.

# Introduction

FinCrime has existed for several decades where criminals carry out unlawful activities for personal financial gains. Given that technology has evolved, criminals are finding new ways to exploit individuals, organizations, and countries. While the evolution of technology has propelled financial activities like funds transfer, there are several risks associated with it. Hence, the challenge of combating FinCrime is becoming more complex each day. By the time governments find such unlawful activities and enforce regulations and compliances, a substantial financial loss may have already occurred. It is important to quickly identify potential suspects and to do this, technological solutions that accelerate data collection in an optimized manner are pivotal.

# Understanding FinCrime

Before we dive into combating FinCrime, it is pertinent to understand the different types. Here are some of the commonly known ones:

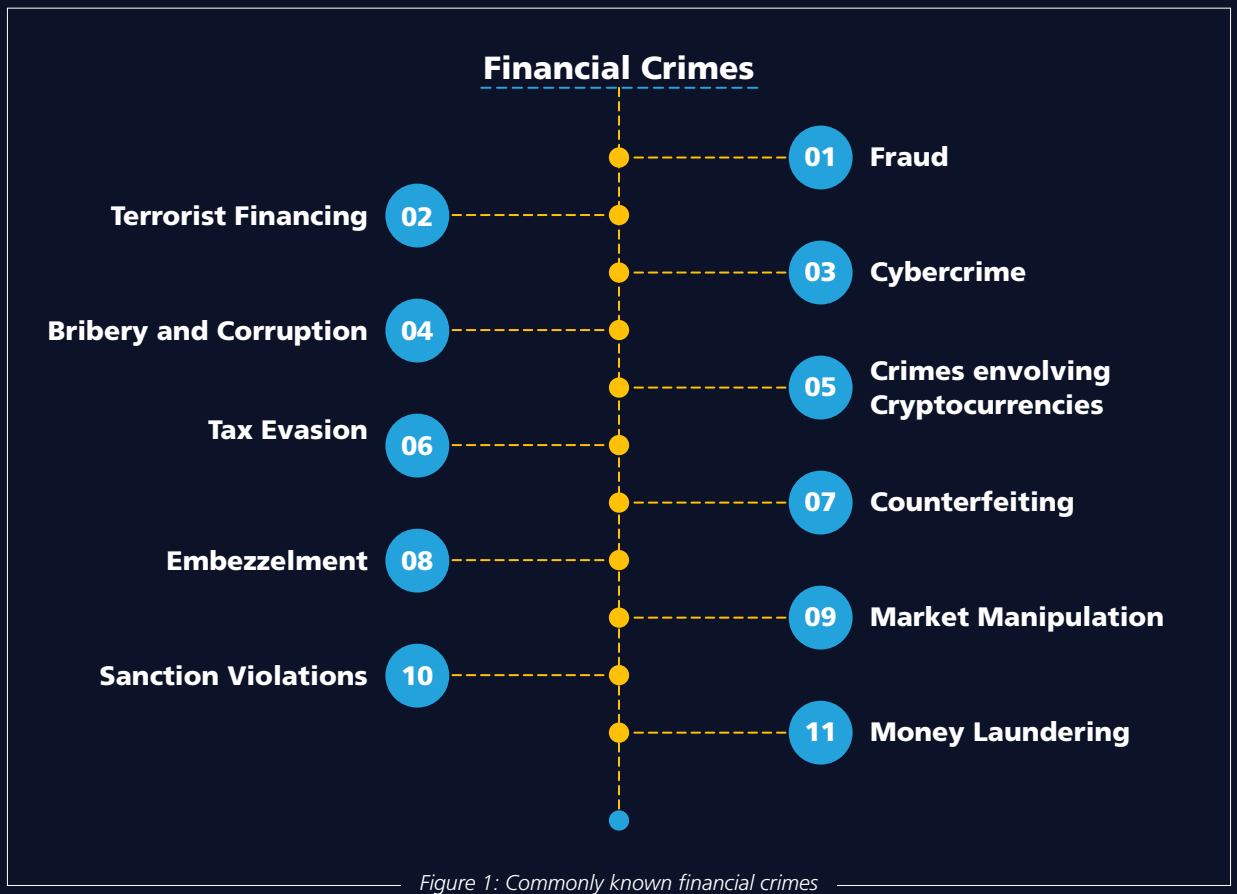


*Figure 1: Commonly known financial crimes*

## 01 Fraud

This is a broad term that covers activities like identity theft, investment/ credit card trickery.

## 02 Terrorist Financing

This refers to the process of collecting funds to support terrorist activities. These funds can be sourced from legitimate or illegitimate means and are often laundered to disguise their intended use.

## 03 Cybercrime

This includes any criminal activity involving computers and networks and can range from hacking and data breaches to online fraud and theft of financial information.

## 04 Bribery and Corruption

Involves offering, giving, receiving, or soliciting something of value to influence the actions of an official or any other person in charge of public or legal duty.

## 05 Crimes involving Cryptocurrencies

This is based on blockchain, which is decentralized and anonymous in nature. It has become a fertile ground of financial crimes internationally due to the anonymity offered.

## 06 Tax Evasion

Refers to act of avoiding paying taxes to a government. It is a deliberate attempt to underreport income or overstate deductions to reduce the amount of taxes owed.

## 07 Counterfeiting

Refers to the creation of fake currencies or similar valuable items. It typically requires expertise and resources.

## 08 Embezzlement

This is a type of theft where a person who is trusted with managing money or property misappropriates it for their own benefit. This often occurs within a business or organization where the individual has access to funds or assets.

## 09 Market Manipulation

Refers to practice of artificially influencing the price of a security, commodity, or currency. This can be done through various methods, often involving deceptive or fraudulent tactics.

## 10 Sanctions Violations

Occurs when an individual or entity engages in financial transactions or other activities that are prohibited by government-imposed sanctions.

## 11 Money Laundering

Involves concealing the origins of illegally obtained money, typically by means of transfers involving foreign banks or legitimate businesses. It is often a secondary crime, facilitating other criminal activities like drug trafficking and terrorism.

# Challenges in Combating FinCrime

With the evolution of technology, financial crimes are growing day by day. Towards this, it is important understand the key challenges:

## 01

**Evolving nature of financial crimes:**
Given that technology is evolving each day, criminals are using advanced methods to evade detection. These include cryptocurrency, dark web etc.

## 02

**Regulatory challenges:**
This includes fragmented compliance frameworks, evolving AML (Anti Money Laundering) laws, cross-border jurisdiction challenges, and data privacy concerns.

## 03

**Technological challenges:**
Many financial platforms still rely on legacy systems. Also, adopting a new technology takes time and finding skilled professionals is an underlying challenge.

## 04

**Digital literacy:**
Newer financial crimes are unknown to many people due to the lack of digital literacy.

## 05

**Data sharing challenges:**
Data sharing regulations vary across departments, making it difficult to share information on-demand.

# Trends in FinCrime

FinCrime is a multifaceted challenge, with new threats emerging all the time. This is further amplified with the growth of new technologies. Below are the latest trends.

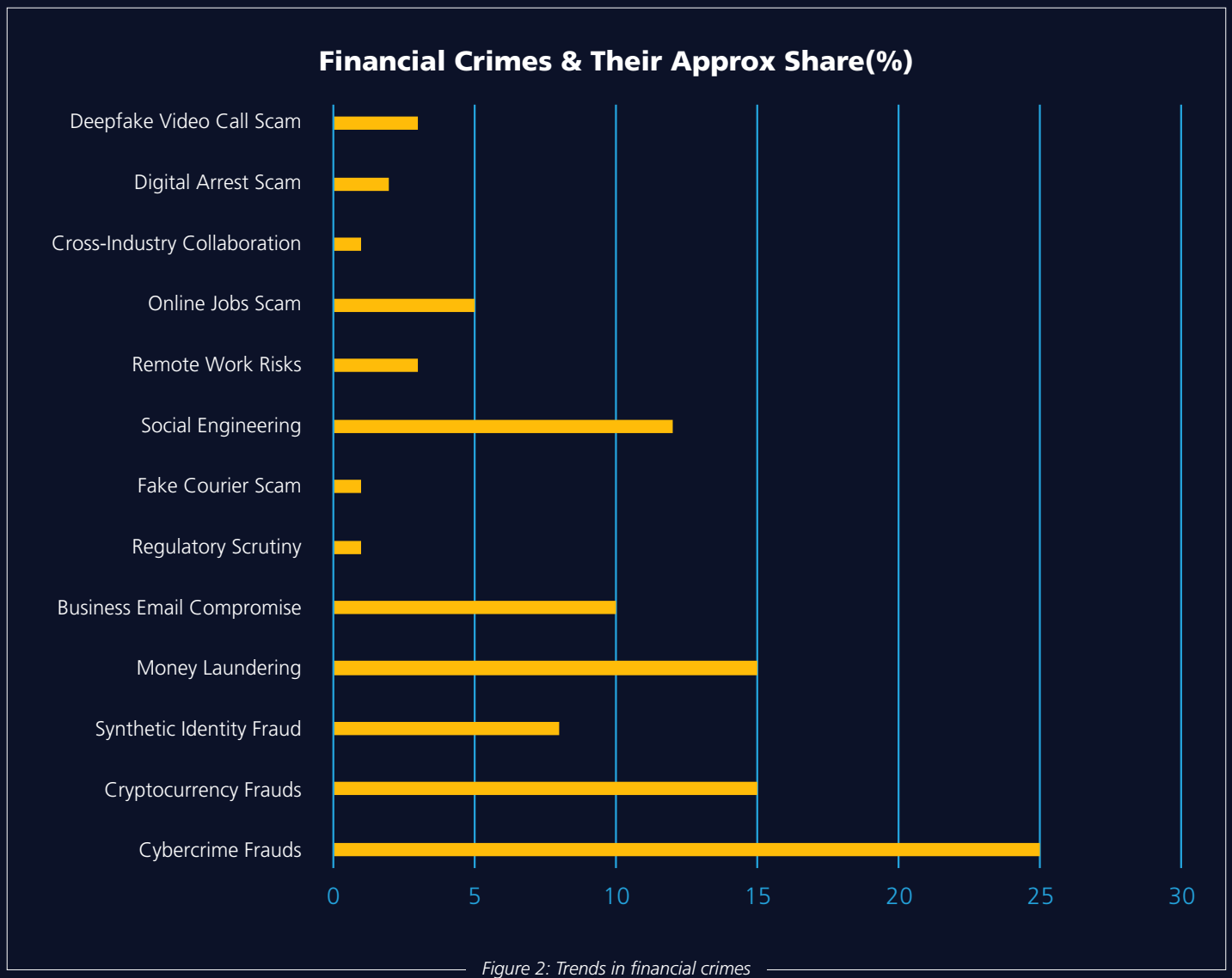


*Figure 2: Trends in financial crimes*

# Impact of FinCrime

FinCrime has a significant impact on most entities, ranging from governments to individuals. The following are some of the major impact areas:

### Economic Impact

- Significant economic losses, destabilized markets, and reduced capital availability
- The global cost of financial crime is estimated to be trillions of dollars annually.

### Social Impact

- Individual impact that further weakens private and government bodies
- Social impact leads to instability and reduced confidence in financial systems

### Financial Impact

- Direct loss from financial crimes, such as fraud and cyber attacks
- Increased compliance costs, reputation damage, and regulatory penalties

# Solutions to combat FinCrime

While there are solutions available to assist in combating financial crimes, most of them either work in silos or are partial in nature. Some of these solutions have been listed.

- AI/ ML- based fraud detection
- Transaction monitoring systems
- Identity verification and authentication solutions
- AML solutions
- Regulatory and compliance technologies
- Cybersecurity and threat intelligence solutions
- Blockchain and cryptographic solutions
- Insider threat and fraud prevention
- Open banking and application programming interfaces (API) security
- Inter-industry and government collaboration

The above solutions have challenges like data quality/ format issues, integration problems, weak endpoint security, excessive alerting, delayed investigations, regulatory complexities, legacy systems etc. However, these challenges are interconnected, and solving them requires a combination of technology, regulation, and industry collaboration. Therefore, we propose a custom solution that drives innovation by strategically leveraging technology to achieve optimal outcomes.

# **FinSafeX -** Proposed solution to combat FinCrime

Financial crimes are evolving, and a combination of technologies is required to combat them effectively. A multi-layered approach integrating real-time monitoring, advanced analytics, and regulatory compliance ensures better fraud detection and prevention. Towards this, FinSafeX comprises robust tools and technologies to collect and process data and generate meaningful reports for use by law enforcement agencies.

## Solution overview

**AI & ML**

- Detects patterns and anomalies in transaction data, enabling early detection of suspicious activities and fraud via AI and ML models.
- Provides insights analyze data and related patterns. As a result, decision-making becomes faster.

**Web Portal**

- Provides an interface for financial institutions to submit suspicious financial information about entities.
- Financial institutions report such data to governing bodies for timely analysis and corrective action via web portals.

**Data Analytics**

- Processes large volumes of data to identify trends and suspicious activities.
- Predicts and prevents financial crimes by analyzing data to generate risk scores based on business rules. Also, suggests law enforcement agencies that will take up the case.

**APIs**

- Facilitates connections with external systems to retrieve data related to a suspect.
- Enables access to reliable external sources, providing accurate information about the individual and establishing seamless data sharing between trusted systems.


*Figure 3 – Technologies of FinSafeX*

## Detailed Solution Architecture

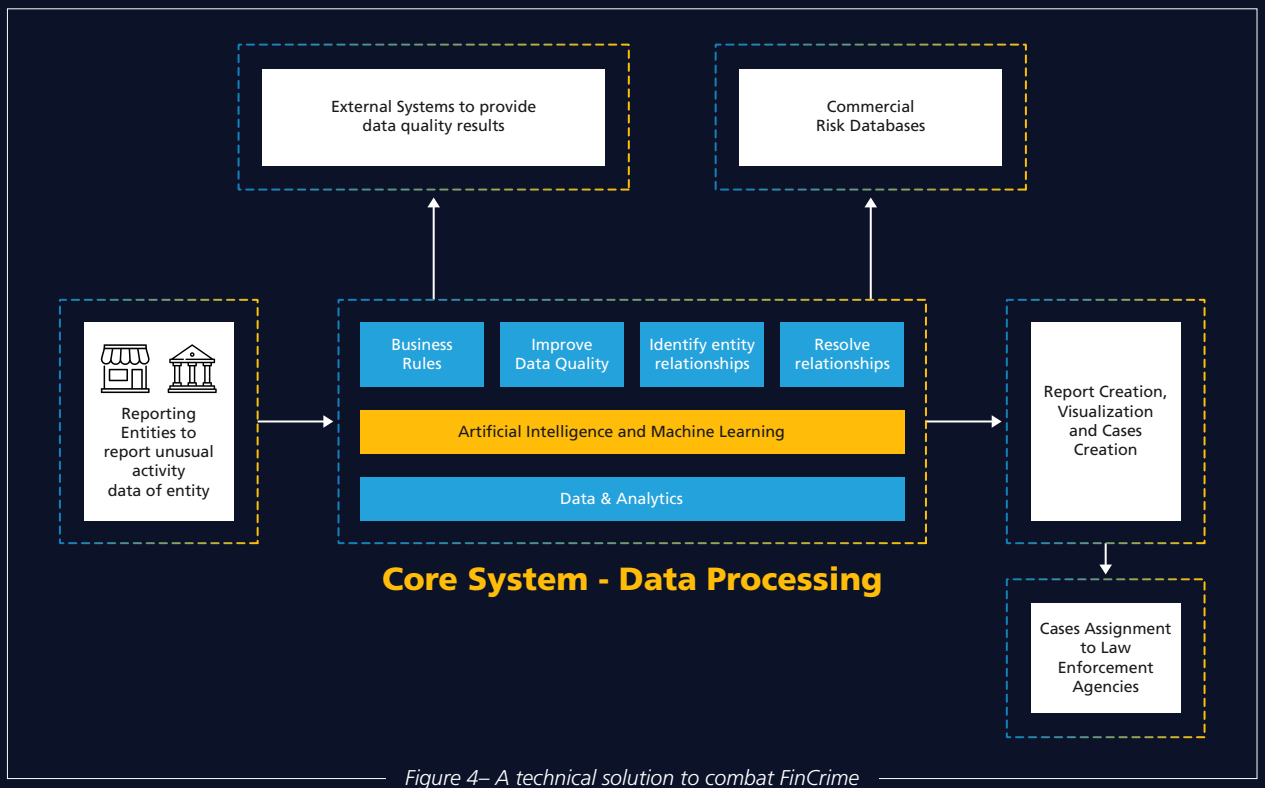


*Figure 4– A technical solution to combat FinCrime*

As shown in the diagram, a governing body can use this approach to intelligently track suspects. It comprises:

- A core system owned by the governing body that collects the data from different reporting entities such as banking institutions.
- The core system is bundled with set of business rules and connects with third-party systems via APIs to improve data quality. It is essential to build relationships and resolve them through an intelligent processing engine powered by AI/ ML.
- Finally, a comprehensive report is generated with the data and an interactive visualization can be created for better analysis. This is then routed to the respective law enforcement agency for further action.

The detailed architecture comprises the following components:

- External systems to report data-
  - Use of APIs for data exchange
  - Using of portal-based interfaces to easily submit financial data

- Physical security of interfaces via hardware security tools.
- Using API gateways to protect the backend services from suspicious traffic.
- A core processing engine that runs business rules to filter out fine-grained data.
- Any suspect's data must be enriched from different agency databases for identification precision.
- There may be different internal systems that process at different levels to dispose the fine-grained information. All such systems must be connected via APIs as the open standard to share the data.
- The case generation tool creates reports for suspicious entities, which is then disseminated to respective law enforcement agencies.
- Visualization tools enable the creation of interactive dashboards, facilitating quicker decision-making through efficient analysis.

Below is the reference solution architecture:

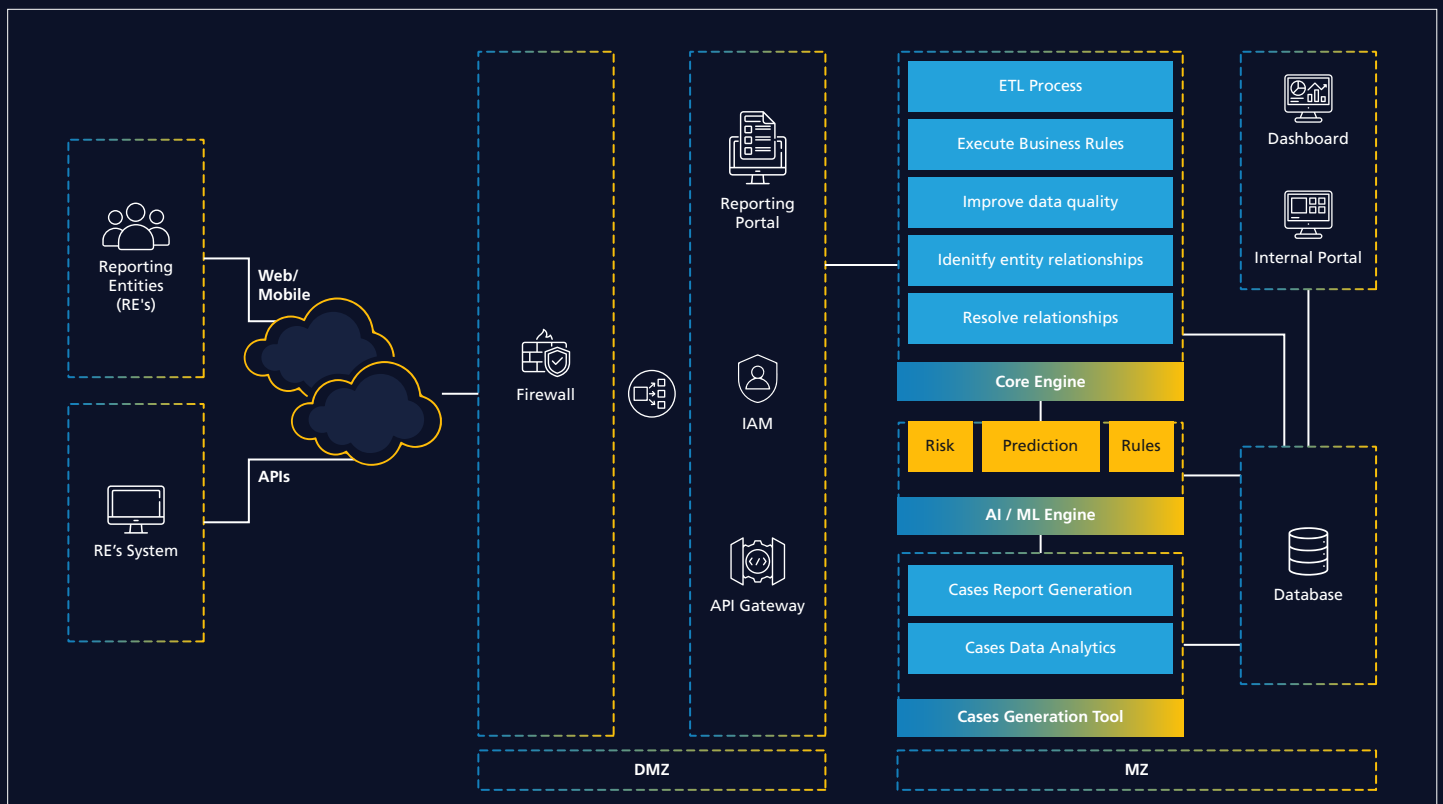


*Figure 5– Reference architecture to build systems that combat FinCrime*

## Solution Outcome

- ~2 TB of data processed in 6 months.
- Simplified reporting helped in increasing the monthly report counts.
- Enhanced the user experience through a new portal for reporting entities and law enforcement agencies.
- API-based connectivity provides real-time data as opposed to SFTP (Secure File Transfer Protocol)-based processes.
- Access to important notifications via a mobile app
- Key information about the reporting format, API integration, and guidelines, which is easily accessible on the portal.

## Value addition

In addition to designing FinSafeX, LTIMindtree has enhanced its value by developing various other tools. Below are some key contributions that have improved the overall system's efficiency.

### Negative News Screening Tool

These tools can be developed to check if a suspect's detail is available in the media. If found, the case will be stronger to verify the suspect. Initially, we define a list of tags related to the negative impression of an individual/ company. We then reach the media digitally to filter out responses as per the requirement. APIs can be used to fetch the data and enrich the main system periodically.

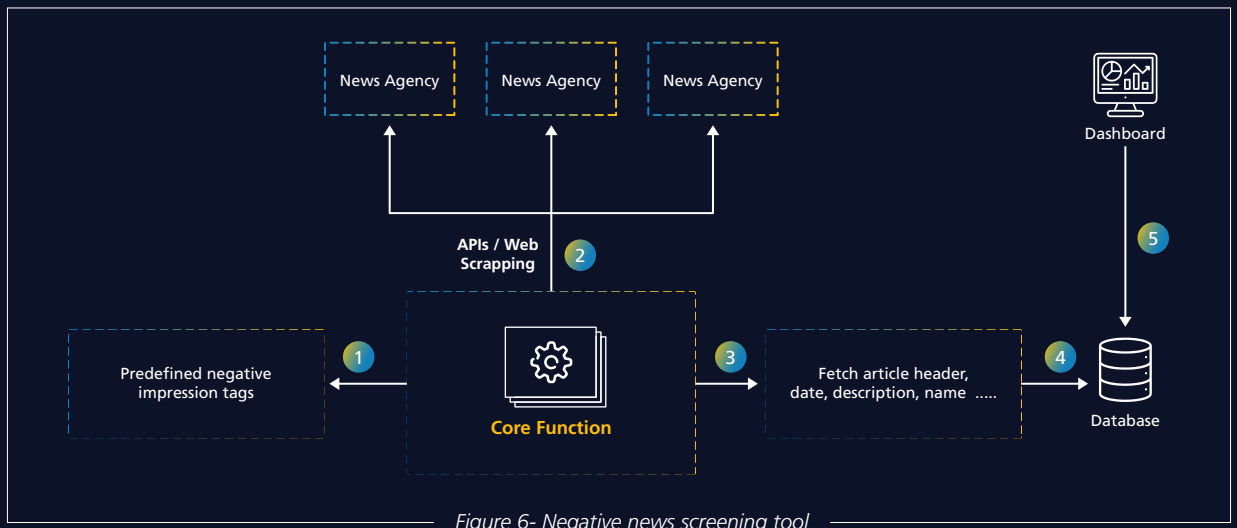


*Figure 6- Negative news screening tool*

## IP Address Screening Tool

Open-source tools are available to find the details of an individual via IP address as location (latitude, longitude), city, region, country, organization, postal code, time zone etc. These can be leveraged to create screening tools for real-time information on a suspect. Additionally, geo-mapping of the address can also be performed in the map via a single or multiple IPs. All such information is available in a single window for faster analysis and decision-making.

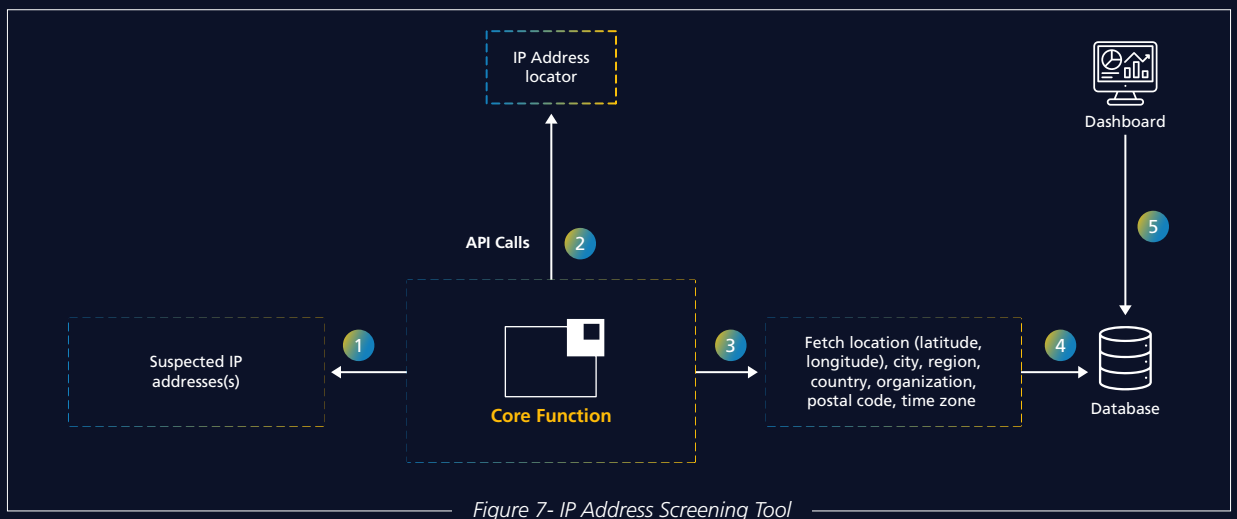


*Figure 7- IP Address Screening Tool*

## Financial Flow Analysis Tool

This tool can help in the analysis of the financial data of an individual through their records like bank statements etc. It facilitates the granular analysis of an individual's financial journey by providing transaction trends and generating interactive dashboards. Analysts can use this information to make decisions, translating to stronger evidence.

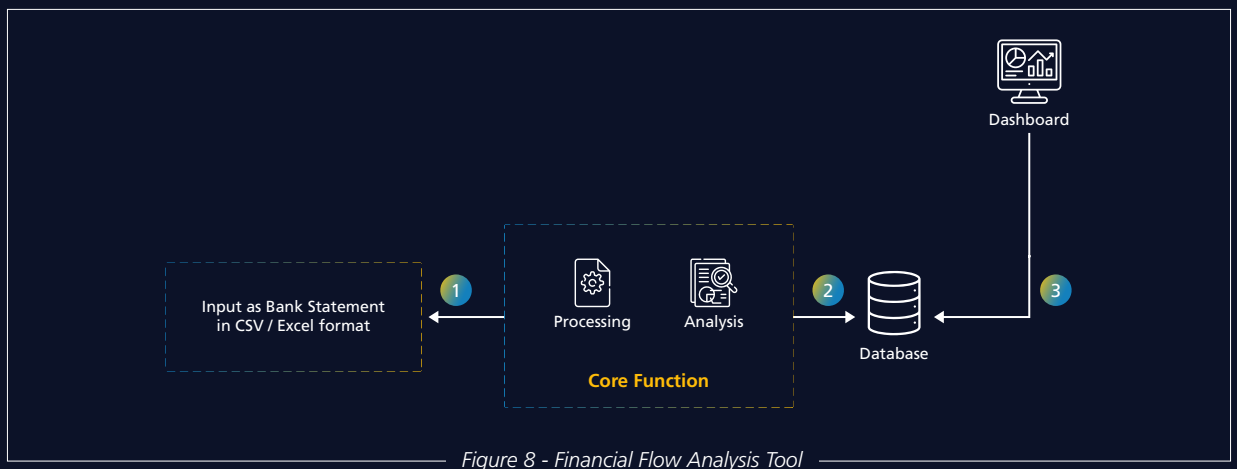


*Figure 8 - Financial Flow Analysis Tool*

## On-demand Data Request Tool

Every organization working towards combating financial crimes has centralized databases where all the records are available. While some information requires a refresh after a certain period, the data repository grows each day. The purpose of an on-demand data request tool is to rapidly search for information from the repository and provide it whenever required.

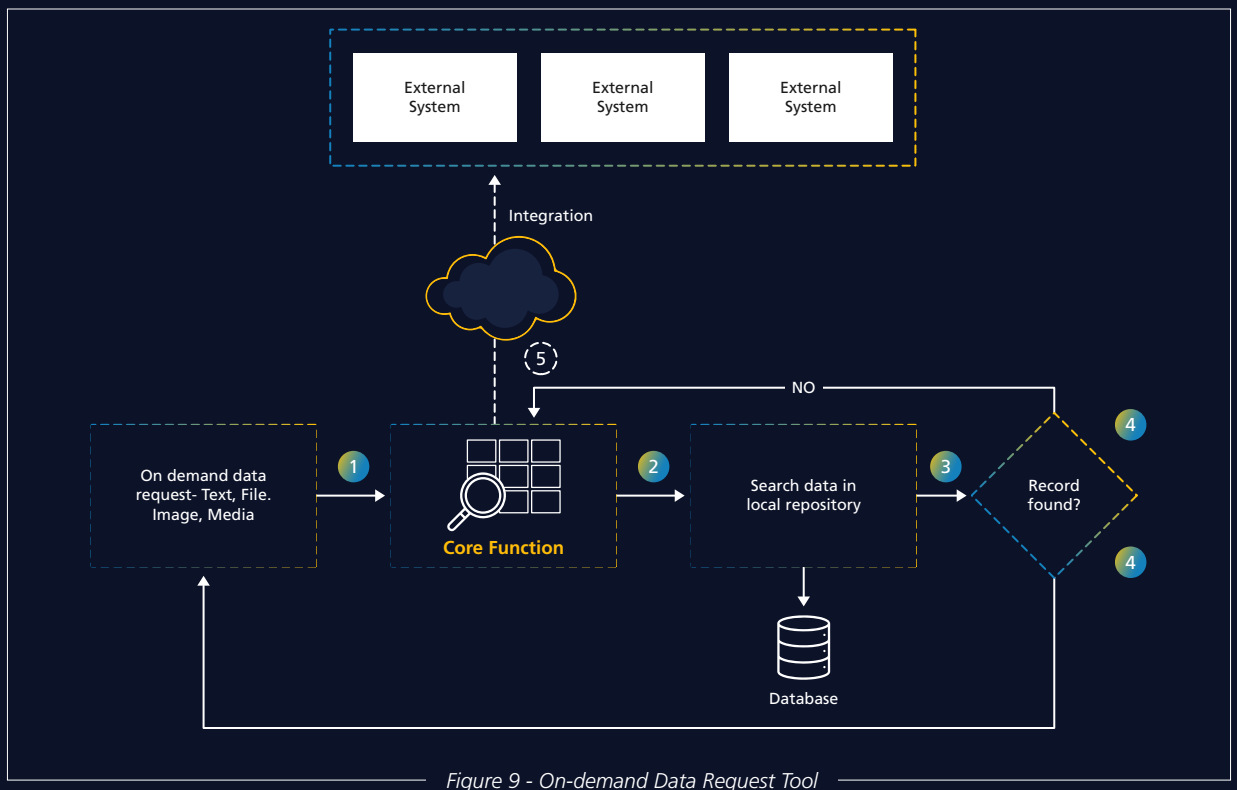


*Figure 9 - On-demand Data Request Tool*

# Conclusion

The future of preventing FinCrime lies in advanced technologies, international cooperation, and continuous regulatory evolution. Innovations in AI, blockchain, and data analytics will play a crucial role in identifying and preventing such crimes.

## Recommendations

- Enhancing cross-border collaboration among regulatory bodies, financial institutions, and law enforcement agencies.
- Financial institutions should invest in robust technologies to improve detection and prevention capabilities.
- Promoting a strong compliance culture within organizations to ensure adherence to regulations and ethical standards.
- The role of whistleblowers in uncovering large-scale financial crimes.
- Timely investments in technology.
- Evaluation and early adoption of technology can save time, cost and effort.
- Continuous monitoring and scope for improvement in existing systems.

By understanding and addressing the complexities of FinCrime, relevant stakeholders can work together to create a safer and more stable global financial environment.

# Appendix

## References


Redefining Financial Crime Prevention: Cutting-Edge, Subhasis Bandyopadhyay, Sagar Sinha, Mindtree, January 2022

*https://investorsarchive.ltimindtree.com/insights/resources/redefining-financial-crime-prevention-cutting-edge*

Global Framework for Fighting Financial Crime, Deloitte, June 2023

*https://www.deloitte.com/global/en/Industries/financial-services/research/gx-global-framework-for-fighting-financial-crime.html*

Financial Fraud Up as 59% of Indian Firms Faced Crimes in Past Two Years, Abhijeet Kumar, Business Standard, December 2024

*https://www.business-standard.com/economy/news/financial-fraud-up-as-59-of-indian-firms-faced-crimes-in-past-two-years-124121800678_1.html*

Country Performance in Fighting Financial Crime: A Comparative Study 2021, John Cusack, Financial Crime News, October 2021

*https://thefinancialcrimenews.com/country-performance-in-fighting-financial-crime-a-comparative-study-2021-by-fcn/*


## Acronyms

| Sr. No. | Abbreviation | Full Form |
|---|---|---|
| 1 | AI | Artificial Intelligence |
| 2 | AML | Anti Money Laundering |
| 3 | API | Application Programming Interface |
| 4 | DMZ | Demilitarized Zone |
| 5 | ETL | Extract Transform and Load |
| 6 | FinCrime | Financial Crime |
| 7 | ML | Machine Learning |
| 8 | MZ | Militarized Zone |
| 9 | RE | Reporting Entity |
| 10 | SFTP | Secured File Transfer Protocol |

# Author Profiles


## Dr. Mohan Kumar

*Senior Director of Software Engineering - LTIMindtree*

*https://www.linkedin.com/in/dr-mohankumar/*


Dr. Mohan Kumar is a seasoned delivery leader with over 25 years of extensive experience in the IT industry, specializing in the Banking and Financial Services sector. Currently serving as Senior Director and Delivery Partner at LTIMindtree, he oversees major accounts and drives large-scale digital technology transformation programs. With a Ph.D. in Machine Learning, Dr. Kumar combines deep technical expertise with strategic foresight, staying ahead of modern technology trends and fostering strong partnerships within the ecosystem. As a recognized thought leader, he actively contributes to shaping the future of technology in IT services and consulting, ensuring impactful and sustainable innovation in the financial domain.


## Kumar Gaurav

*Associate Principal - Software Engineering, LTIMindtree*

*https://www.linkedin.com/in/k10gaurav/*


Kumar is a seasoned middleware architect and certified professional specializing in open-source technologies, with a primary focus on WSO2. With extensive experience in the finance and healthcare sectors, he designs and implements robust API management and integration solutions that enhance security, reliability, and cost efficiency. His expertise spans digital transformation initiatives, where he plays a key role in development, optimizing deployment workflows, enhancing production support, and driving innovation in both on-premises and cloud-native applications. Kumar's contributions have led to resilient system architectures and significant performance advancements.