CO-EVOLVING FORENSIC MODELS FOR NEW AGE FRAUDS AND INVESTIGATION

-Vishal Narula & Gaganpreet Puri

Abstract

As the business landscape evolves, organizations face a dual challenge: the rapid emergence of disruptive technologies and the escalating threat of fraud. In response, a strategic and forward-thinking approach is essential. To address these challenges, the co-evolution of forensic models becomes crucial for businesses across industries. The convergence of risk management, data-driven insights, and transformative practices presents a unique opportunity to fortify organizations against potential vulnerabilities and safeguard value and trust.

The Strategic Integration of Forensic Models

In our extensive experience, we have observed that often organizations contemplate integrating forensics into their business at a later stage in their growth journey. However, several compelling factors emphasize the strategic importance of the implementation of forensics in their organizations:

- When it is required by law
- When investors mandate it (for their compliance which is also usually driven by law)
- When it is required by contract with third parties (whistleblowing)
- When an organization suffers from incidents which necessitate such measures
- When faced with myriad situations from evolution in technology and economic conditions.

Mitigating Vulnerabilities through Forensic Integration

During the process of developing business workflows or conducting comprehensive audits, it is customary for many of us to focus on identifying potential pitfalls within well-established processes. Within this context, we diligently examine various scenarios that may lead to adverse outcomes and detrimentally impact the business. Through our rigorous risk assessment methodology, we gain invaluable insights into mitigating these vulnerabilities and effectively fortifying the organization against potential losses.

These very approaches find prominent application in the arsenal of risk management professionals, being instrumental components of meticulous risk assessments that fundamentally shape the formulation of robust control frameworks across organizations.

Internationally acclaimed risk management frameworks adhere to a meticulous process that places the utmost emphasis on the integrity of individuals responsible for critical business functions, as well as the independence of those entrusted with the vital roles of risk management and corporate governance oversight.

While undeniably effective, it is worth noting that these approaches occasionally encounter challenges in terms of agility, hindering their seamless growth and adaptation alongside the evolving business landscape and the dynamic shifts within the economic and regulatory realms.

Given the rapid, break-neck pace at which businesses are evolving today, policies and

processes become outdated within remarkably short spans of time. Consequently, fostering an environment that effectively shields businesses from the perils of fraud calls for the indispensable integration of forensic models, harmoniously co-evolving alongside the very fabric of the business.

Achieving this paramount objective is contingent upon the meticulous incorporation of fraud detection and prevention mechanisms into the very core of building processes. Among the cardinal principles of process development, including efficiency, economy, and speed, lies the indispensable tenet of safeguarding against fraudulent activities, thus culminating in a harmonious and fortified business ecosystem.

Indeed, the absence of forensic processes within an agile environment would run counter to intuition. It would be akin to equipping a propeller plane with a jet engine without reinforcing the aircraft's structure, only to witness its disintegration as soon as it attempts to take flight. Therefore, in an era of rapid evolution, integrating robust forensic processes becomes imperative to ensure seamless growth and resilience against potential vulnerabilities.

Today, we have entered the era of co-evolving forensic models in tandem with the process-building journey. We find technology-driven businesses as the primary protagonists at the forefront of this transformative period. These enterprises are compelled to navigate an ever-changing landscape of digital advancements and data-driven insights, leaving no room for complacency, and demanding a perpetual commitment to adaptability.

In this context, fostering a symbiotic relationship between forensic models and business processes is pivotal for embracing the potential and challenges of this dynamic era.

Prominent Applications of Forensic Models

Within the diverse spectrum of organizations, irrespective of industry, size, or scale, there exist pragmatic avenues through which preventive measures can be embedded to safeguard against fraud. These very approaches can be perceived as essential means of co-evolving forensic models, harmoniously aligning with the ever-changing dynamics of the business landscape.

As we explore these strategies, it becomes evident that they empower businesses to fortify their defences and proactively shield themselves from potentially fraudulent activities.

- **Forensics lens in product designing** – The pursuit of creating and enhancing stakeholders' value lies at the core of most businesses. As technological advancements underpin their operations, comprehending the vulnerabilities that accompany such progress becomes imperative. The efficacy of products and services hinges on how internal and external stakeholders' access and leverage data. Consequently, the integration of forensic models within the product designing process instils a sense of credibility, imbuing these offerings with inherent safeguards to protect all users and consumers. By proactively addressing potential risks, organizations can bolster customer trust and fortify their market position.

- **Forensics lens in process formation** – While adopting a risk-conscious approach and establishing controls to mitigate potential risks is a commendable practice, the true differentiator lies in the continuous monitoring of data through a forensic lens. This approach yields invaluable insights that drive process reimagining, enabling

businesses to adeptly detect and prevent fraud and abuse. By proactively safeguarding against threats, organizations can avert value erosion and pre-empt regulatory challenges that may arise due to insufficient vigilance. Embracing this proactive stance empowers businesses to navigate the ever-changing risk landscape with confidence and resilience.

- **Penetration testing of controls** – Adopting a proactive stance in scrutinizing controls through 'Red-Flags' testing yields transformative insights, facilitating process and policy enhancements to address known risks. A methodology akin to 'Ethical Hacking' or 'Penetration Testing' empowers organizations to embrace an objective perspective, untainted by confirmation bias, as they rigorously assess their resilience against fraud and abuse. By leveraging such an approach, businesses can confidently strengthen their defences and proactively safeguard their assets, ensuring heightened protection against potential threats and vulnerabilities.

In the forthcoming landscape, the prominence of organized fraud against industries is likely to escalate. Consequently, fostering a collective imperative for knowledge exchange and comprehension about syndicated frauds that exert a significant impact on businesses becomes extremely important. By collaboratively disseminating insights and understanding, industries can fortify their defences, cultivate resilience, and proactively combat the rising tide of sophisticated fraudulent activities.

A few thoughts on how an organization could safeguard itself and its customers / subscribers from organized fraud:

A) Making regulatory databases accessible to industry participants:

Granting businesses in the fintech and e-commerce domains access to regulatory databases would prove highly advantageous. By leveraging such access, these companies can effectively safeguard themselves and their valued customers from fraud and abuse occurring on their platforms. The establishment of a safer digital transacting environment contributes to expediting the realization of financial inclusion goals. By fostering a more reliable and trustworthy digital financial system, this approach serves to identify and restrict bad actors, ensuring that they are not able to exploit the vulnerable in the digital financial ecosystem.

Organizations operating within the direct-to-consumer, FMCG and pharmaceutical sectors stand to achieve accelerated consumer reach through heightened trust in the digital consumer economy. This augmented trust fosters an environment conducive to enhancing the quality and convenience of service delivery to consumers, thereby propelling a faster and more transparent economy. The convergence of these factors presents an unparalleled opportunity for businesses in these spaces to unlock unprecedented growth and cultivate lasting customer relationships, all while contributing to the dynamic evolution of the digital ecosystem.

B) Industry associations facilitating the collation of data of persons causing fraud and abuse:

Industry associations hold a pivotal role in fostering a robust economy by orchestrating collective industry participation. Empowered by substantial contributions from industry stakeholders, these associations can spearhead the establishment of databases or systems

dedicated to collating crucial information on bad actors. By cultivating such shared repositories, industry bodies can pave the way for decisive action against fraudulent elements, bolstering the integrity of the business landscape and engendering a more secure and sustainable economic environment. Through collaborative efforts, these associations become instrumental in fortifying the industry's resilience against illicit activities and promoting a culture of trust and accountability.

Efficiently seeking regulatory and law enforcement interventions to safeguard consumers hinges upon the collective collaboration of industry participants in nurturing safer economies. By joining forces and aligning their efforts, businesses can amplify their advocacy for impactful regulatory measures, fostering an environment that prioritizes consumer protection and trust. This united front empowers industry stakeholders to proactively address challenges, capitalize on opportunities, and drive transformative change, ultimately cultivating economies that thrive on the principles of safety, transparency, and sustainable growth.

Amid the advent of disruptive technologies, the collaboration between technology developers and those building products and services on these technological advancements becomes paramount. Together with seasoned forensic professionals, they must proactively tackle the risk of fraud to safeguard the integrity and trust within future digital economies. This strategic partnership will be instrumental in preventing any erosion of value and confidence, paving the way for sustainable growth and continued innovation. By forging these interdisciplinary alliances, businesses can confidently embrace the vast potential of disruptive technologies while nurturing an environment that upholds the principles of security, transparency, and mutual trust.

By embracing a forward-thinking mindset and drawing insights from successful practices, these companies can effectively navigate the dynamic landscape and capitalize on emerging opportunities.

Future of the fight against fraud and abuse

The responsibility of safeguarding against fraud will no longer rest solely on the shoulders of risk professionals. Instead, it will evolve into a collective responsibility, shared by stakeholders across the entire value chain, spanning from development to operations.

This transformative shift signifies a paradigmatic change in the approach to fraud prevention, as organizations embrace a comprehensive and integrated strategy, intertwining risk mitigation measures seamlessly throughout their business lifecycle. By fostering a culture of shared ownership and vigilance, businesses can effectively fortify their defences against fraudulent activities, safeguarding value and trust in the journey ahead.

We anticipate organizations to undergo a profound shift in their behaviours, transcending the traditional notion of "if it's not broken, don't fix it." Instead, we envisage a proactive paradigm where businesses embrace a more predictive approach to decision-making.

By effectively anticipating and pre-empting potential challenges, companies can position themselves at the forefront of innovation, driving transformative change, and sustaining their competitive edge. This shift in mindset is pivotal for organizations to thrive in the face of evolving complexities, adapting with agility, and fostering

a culture of continuous improvement and foresight.

Navigating the future landscape

In this era of transformative change, organizations must act decisively to co-evolve forensic models and bolster their defences against fraud. By embracing a predictive mindset and forging collaborative partnerships, businesses can navigate uncertainties with

confidence and adapt seamlessly to dynamic landscapes. The journey towards safer and more resilient economies requires a collective effort, and together, organizations can thrive and drive progress in the digital era.

About the Authors:

Mr. Narula specializes in managing un-precedented situations and has led some of India's highest-profile investigations into complex accounting frauds and financial misstatements, anti-trust and anti-competition matters and headline-making bribery and corruption cases. He has extensive experience providing expert testimony in commercial arbitrations and litigations in India and abroad.

Mr.Puri is a Managing Director with Alvarez & Marsal Disputes and Investigations in New Delhi. As the leader of the Risk and Regulatory practice in India, he has experience with financial statement fraud, embezzlement and asset misappropriation, bribery and corruption, diversion of funds, economic offences, trade sanctions, regulatory non-compliance, and code of conduct violations.