Platforms: The new frontier of fraud in India

PwC's Global Economic Crime and Fraud Survey 2022: India Insights

pwc

Table of contents

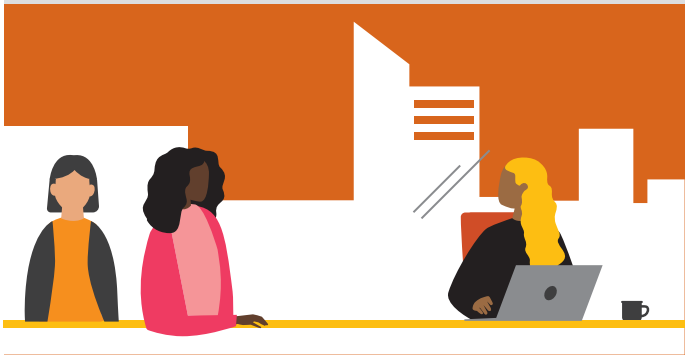
1

About the Survey

The second edition of PwC's Global Economic Crime and Fraud Survey 2022: India Insights looks at the new frontier of economic crime – platform fraud, or fraud associated with social media, enterprise, e-commerce and other kinds of platforms. Largely unrecognised for years, this insidious form of fraud has become more common since the start of the pandemic, owing to the rise in remote work and growth in e-commerce, delivery applications and contactless payments. And it is evolving and growing at a worrying pace, posing a new set of challenges for Indian companies.

For the second report in this series, PwC surveyed 111 organisations across India from diverse industries such as technology, financial services, banking and capital markets, consumer products and retail, education, healthcare, hospitality and leisure, and industrial products and manufacturing.

1. PwC surveyed 111 organisations across India from diverse industries.
2. Amongst those surveyed, 71% belonged to the C-suite.
3. Half the companies had a turnover over USD 1 billion.



A snapshot of the previous edition of PwC's Global Economic Crime and Fraud Survey 2022: India Insights[1]

What is the financial impact of fraud or economic crime on Indian organisations?

40%
of Indian organisations lost between USD 50,000–1,00,000.

17%
lost between USD 1 million–50 million.

5%
incurred a loss of USD 50 million and above through the most disruptive incidents of fraud/crime.

The India highlights of the survey reveal that…

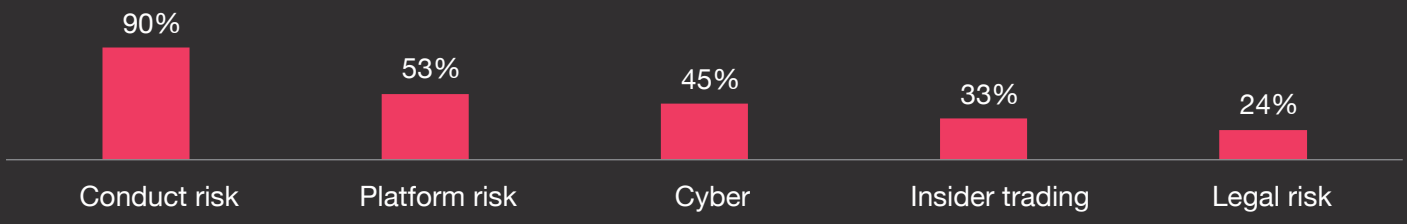
95% of companies experienced new fraud incidents due to COVID-19 disruptions.

60% of companies with global annual revenues of USD 1 billion or more experienced fraud over the last 24 months.

52% of companies experienced fraud or economic crime in the last 24 months.

67% of companies that experienced fraud reported that the most disruptive incidents came via external attacks or collusion between external and internal sources.

Categories of fraud, corruption or other economic/financial crime faced by Indian organisations in the last 24 months:



Tackling fraud and economic crime – creating innovative solutions to new and emerging threats

Organisations are strengthening internal controls, technical capabilities and reporting to defend against external predators. To shore up their perimeter, they must:

1. understand the end-to-end life cycle of customer-facing products
2. strike the proper balance between user experience and fraud controls
3. orchestrate data.

1 https://www.pwc.in/assets/pdfs/consulting/forensic-services/pwcs-global-economic-crime-and-fraud-survey-2022-v3.pdf

2

Platforms: An insidious fraud frontier

Our survey reveals that organisations in India are grappling with various types of platform fraud, as platforms became an integral part of the way they conduct business. Social media platforms connect us every day. Ecommerce platforms provide access to goods and services. And enterprise platforms help companies interact with customers, process transactions and move funds. On average, organisations operate five platforms in the normal course of business vis-à-vis the global average of four.

Platform fraud isn't new. In the banking industry, it has been referred to as financial crime for decades. However, growth in the number of platforms used during the pandemic and new modes of instant payment have dramatically increased the risks associated with platform fraud.

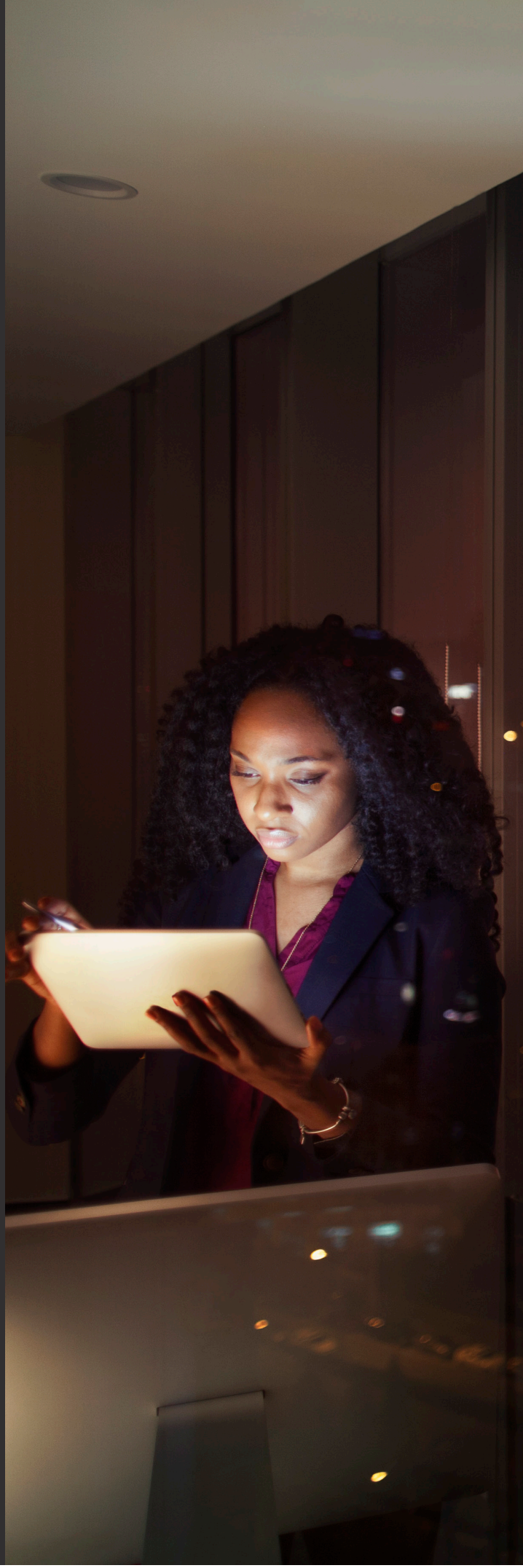
This report aims to not only make Indian companies aware of risks associated with platform fraud, but also help them leverage fraud prevention and detection strategies and tactics already in their toolkits.

5 platforms are now operated by the average organisation in India.

During the pandemic, Indian consumers and organisations were quick to adopt new platforms. Today, an average Indian company operates five platforms in the normal course of business. As a result, the incidence of platform fraud is a lot higher in India.

Puneet Garkhel, Partner – Risk Consulting and Leader – Forensic Services

---



3

The rise of platform fraud

For several years now, there has been a shift towards platforms as a mode of conducting business. The pandemic-induced lockdown only accelerated that shift. Since then, there have been several innovations around platforms, as organisations, both large and small, were forced to shut offices, stores and showrooms and switch to home delivery models and contactless payments.

This new way of doing business exposed Indian organisations to new kinds of risks. Our survey found the incidence of platform fraud to be considerably high in India – 57% of all fraud incidents in India were platform fraud.

57%

of all fraud incidents in India were platform fraud.

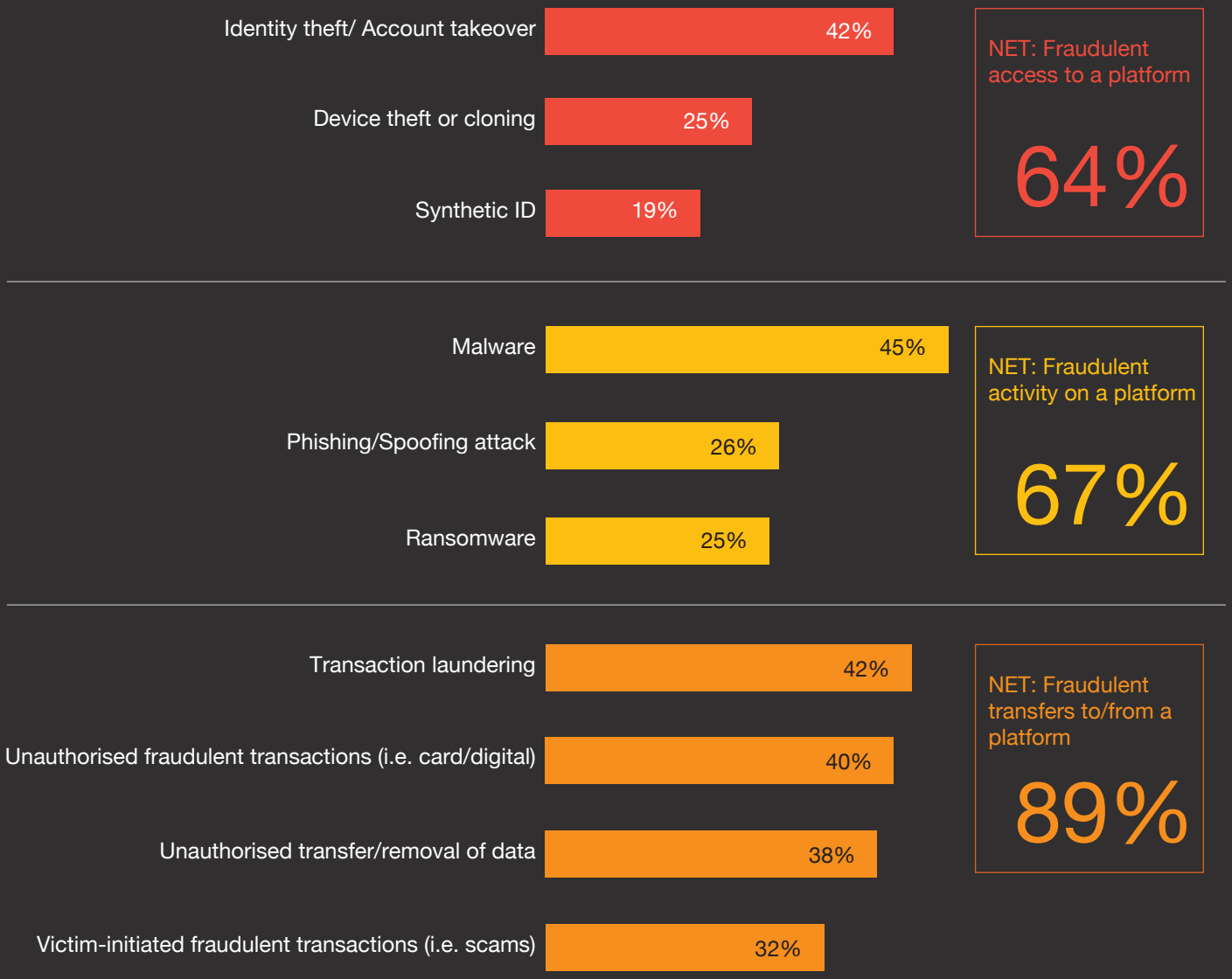
4

What platform fraud looks like

Fraudulent access to platforms can take place across multiple entities such as social media, knowledge, media sharing, services and goods platforms. Such fraud accounted for 64% of platform fraud in India. The unfamiliar and innovative nature of platform fraud is a key reason behind a general lack of understanding among business leaders about their risk exposure to this fraud category.

Over three quarters of organisations state platform fraud resulted from a fraudulent transfer to/from a platform

How platform frauds were executed



Enterprise platforms are most likely to be the site of malware, phishing, money laundering and ransomware incidents. Ransomware, in particular, has grown into a dangerous threat with the potential to inflict catastrophic damage.

In 2022, two large Indian pharmaceutical companies fell prey to a ransomware attack, followed by data leaks. Two different ransomware groups put up the companies' confidential information on a dark web forum.

Of those organisations that experienced frauds across their financial platforms, fraudulent transfers to/from a platform constituted 89% of all platform frauds in India. The tactics adopted by fraudsters range from basic unauthorised digital purchases – for instance, from stealing a credit card number to buy goods and services to more complex schemes such as identity theft and 'triangulation' fraud (this happens when a fraudster hijacks the e-commerce buying process).

In mid-2020, a major Indian conglomerate faced a triangulation fraud. It had launched a retail platform to sell groceries across various categories to help consumers shop during the pandemic. Fraudsters developed fake websites that resembled the platform, thereby cheating consumers and causing reputational damage to the Indian company.

There are several types of customer fraud as well. Payment frauds – which involves credit cards and digital wallets – made up 92% of all customer frauds in India. Impersonation, authorised push payments, application/ lending fraud and claims/dispute fraud are some of the other ways in which customers get defrauded.

5

Underestimating the threat

Newer entrants to the platform environment face an increased risk as fraud perpetrators have become more sophisticated. Our survey shows that too many business leaders, both providers and users, aren't fully aware of their exposure to platform fraud.

Organisations often don't view platforms as a discrete sector. For instance, a company dealing with five platforms in the normal course of business may not address the grouping as an entity with common risk considerations. Rather, they are treated as five separate vendors, each with its own threat profile.

In the banking industry, for example, organisations have built sophisticated systems over the past two decades to protect assets and customers. But today, as a portion of transaction processing moves away from legacy banks to platforms, the obligation towards security is also transferred – except that many platforms are not as well equipped as banks to identify, prevent and mitigate fraud.

99%

of fraud incidents in the past 24 months have been on one of these platforms:

1. Financial
2. Social media
3. Goods
4. Enterprise
5. Media sharing
6. Knowledge sharing
7. Services

6

Combating platform fraudsters

Platform fraud has opened up a new frontier for fraud and economic crime. Financial gain is the most common motive in platform fraud cases – in India, 44% of perpetrators commit fraud for financial gain. Other motives listed out by organisations were brand damage (32%) and competitive advantage (21%).

Financial platforms were found to be the most vulnerable, particularly those involving fund transfers – 62% of all platform frauds took place on financial platforms. The financial impact of such frauds is just a part of the harm caused to organisations. Damage to the brand and loss of customer loyalty and trust can be far more significant.

But there is hope. With proper security and controls in place, organisations can protect themselves. An understanding of who the malefactors are, where they're coming from, and how they're breaching the perimeter forms the framework for mounting a proper defence. Protecting your business begins with identifying the vulnerabilities along the new frontier.

26%

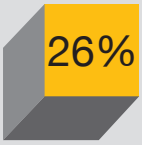
of Indian organisations lost over USD 1 million due to platform fraud.

44%

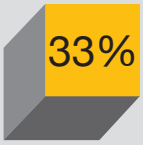
of perpetrators commit fraud for financial gain.

The enemy within: Four out of every ten platform frauds in India were conducted by internal perpetrators. Moreover, 26% of platform frauds involved collusion between internal actors and external perpetrators. This implies that if companies have stronger internal controls in place, over two-thirds of all platform frauds can be mitigated.

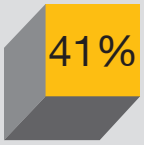
Main platform fraud perpetrators



Collusion between internal and external



External perpetrator

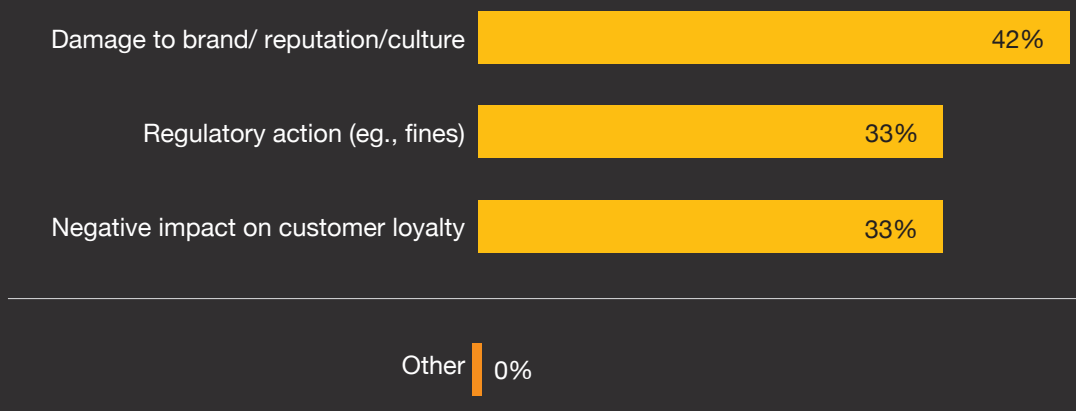


Internal source

Outcomes as a result of platform fraud

Internal outcomes/effects

93%



External outcomes/effects

77%

7

Protecting your perimeter: Identify, assess, execute

Given the rapid pace at which the platform threat environment is evolving, there are several steps companies need to take to protect themselves against this new frontier of fraud.

1

Elevate responsibility for platform risk management to a chief risk officer

Platform fraud requires executive attention and an integrated, enterprise-wide response strategy with a focus on resilience. A C-suite level executive should be responsible for risk control policy. And organisational leaders must guide the risk management programme – particularly when an emerging threat has the potential to upend the business.

2

Stay vigilant for red flags

Risk leaders need to be proactive and design a meaningful strategy to identify, assess and execute a fraud response. Otherwise, the consequences can be devastating. This can be achieved by putting in place a monitoring programme that identifies anomalies and alerts the company. Similarly, corporations need to be aware of a spike in online activity, especially after long periods of dormancy.

Negative media coverage can also provide clues. If platforms form a significant part of your business, it's critical to pay attention to their presence in the news. Be aware of what analysts, consumers and competitors are saying about the platforms you work with, and regularly check watchdog sites for service complaints. Social media monitoring is another important tool to keep you on top of what's happening in the market and alert potential bad actors.

3

Measure, monitor, control

Your customers trust you with their personal data. Conduct a risk assessment to determine your exposure and establish protocols for gaining visibility into the platforms you work with.

Purpose-built transaction monitoring systems are necessary and an effective way to prevent and detect red flags. But depending on your exposure, knowledge of your partners' controls is crucial – perhaps in the form of third-party audit reports.

4

Be risk aware

Sanctions evasion
Fraudsters are increasingly circumventing sanctions in certain jurisdictions to conduct platform fraud – primarily in the financial realm. Stay informed and aware of this risk if you have potential exposure.

Environmental, social and governance (ESG)
Under this broad umbrella encompassing environmental, social and governance issues, rising criminal threats include human trafficking and privacy invasion – by government entities, in some cases, as a cost of doing business.

8

Building resilience to combat platform risk

Given the rapid increase in and growing sophistication of platform fraud, this category of fraud poses a substantial risk to organisations in India. Even though Indian organisations have been undertaking measures to combat fraud for several years now, platform fraud is a dangerous and growing risk. It has emerged as the most aggressive threat of the era – particularly with the pandemic accelerating digital transformation and sparking a sea change in how we conduct financial transactions.

The answer may lie in technology: Respondents to our 2022 survey reveal numerous solutions they're using to combat platform fraud, from document verification and validation to anomaly detection. But wherever this new frontier of fraud and economic crime leads, building resilience into an enterprise-wide risk strategy is the key to protecting your perimeter.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us

Puneet Garkhel
Partner and Leader, Forensic Services
puneet.garkhel@pwc.com

Rahul Sogani
Partner, Forensic Services
rahul.sogani@pwc.com

Atul Luthra
Partner, Forensic Services
atul.luthra@pwc.com

Rohit Goel
Partner, Forensic Services
rohit.goel@pwc.com

Dhruv Chawla
Partner, Forensic Services
dhruv.chawla@pwc.com

Sumit Makhija
Partner, Forensic Services
sumit.makhija@pwc.com

Darshan Patel
Partner, Forensic Services
darshan.patel@pwc.com

Moushumi Vaidya
Executive Director, Forensic Services
moushumi.vaidya@pwc.com

Gautam Dharamshi
Partner, Forensic Services
gautam.dharamshi@pwc.com

Ritesh Khot
Executive Director, Forensic Services
ritesh.khot@pwc.com

pwc.in

Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

KS/February 2023 - M&C 25392