Platform fraud: the new frontier of economic crime

PwC's Global Economic Crime and Fraud Survey 2022

pwc

www.pwc.com/fraudsurvey

The second snapshot from PwC's **Protecting the Perimeter** report picks up at the new frontier of economic crime: platform fraud. Largely unrecognized for years, this insidious form of crime is accelerating and evolving, as the pandemic-era acceleration to ecommerce, delivery, contactless payments and remote work has opened up new avenues of entry for fraudsters.

By identifying platform fraud – essentially, giving it a name for the first time – we aim not only to make companies aware of these risks, but also to help companies leverage fraud prevention and detection strategies and tactics already in their toolkits.

To be clear, platform fraud isn't new. In the banking industry it's been referred to as "financial crime" for decades. But as the prominence and scale of platforms has grown and the means, speed and methods of payments have changed, risk has dramatically increased.

40%

of incidents in the last 24 months are platform fraud.

04

platforms are now operated by the average organisation in the normal course of business.

A perfect storm: The rise of platform fraud

01

Platforms have been an integral part of our lives for years. 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.

In the spring of 2020, platforms became even more critical to consumers and businesses. As the pandemic took hold across the globe, it accelerated the shift already underway toward platforms as a mode of business. Organisations large and small were forced to close their doors, convert to delivery and accept contactless payments. Commerce found a way to keep functioning – but lacking the tech infrastructure to adapt to remote business, many companies turned to platforms.

At the same time, entrepreneurial innovation rushed new or expanded platforms to market to meet the need, and businesses quickly got onboard – in some instances, as a matter of survival.

Of course, any new way of doing business exposes vulnerability to new risks – particularly when the catalyst is a tectonic shift in the business world.

In this instance, fraudsters were quick to find cracks. More than half of organizations experienced some kind of fraud in the past year – and four out of every ten of those incidents were platform fraud, according to this year's survey.

Today's criminals are constantly innovating, continually finding new opportunities to infiltrate gaps in the perimeter.

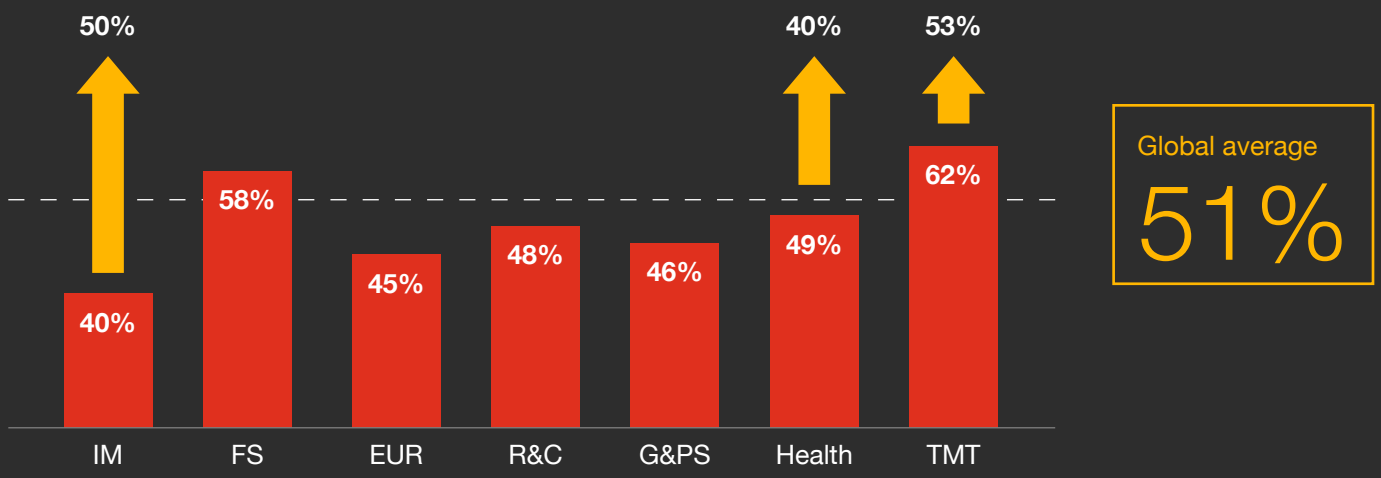
And the numbers are jarring. **Fewer than half of respondents to our survey feel they have a good understanding of their risk profile.** Only a third are confident in their ability to respond swiftly to remediate a fraud event. And perhaps most concerning, just a third believe they have the proper controls in place to prevent fraud in the first place.

How has fraud changed?

51%

of surveyed organisations say they experienced fraud in the past two years, an increase from 47% in 2020 and the highest level in our 20 years of research.

Organisations in the TMT and FS sectors are more likely to report experiencing at least one incident of fraud vs. other sectors



What does platform fraud look like?

02

While PwC's Global Economic Crime and Fraud Survey demonstrates C-suite concern about the rise in platform fraud, business leaders also reveal a general lack of understanding regarding their risk exposure to platform fraud.

Fraudulent transfers to or from a platform are the most common type of platform fraud, comprising more than three-quarters of all incidents. Fraudsters' tactics range from basic unauthorised digital purchases – stealing a credit card number to buy goods and services – to more complex schemes such as identity theft and "triangulation" fraud.

These often include intricate plots such as drop-shipping fraudulently purchased items to "legitimate" customers. Other scams involve creating fake buyers and customers (using stolen identities to obtain goods and services on credit or to prepare for future schemes) and fake sellers and merchants (an exhaust channel for stolen cards).

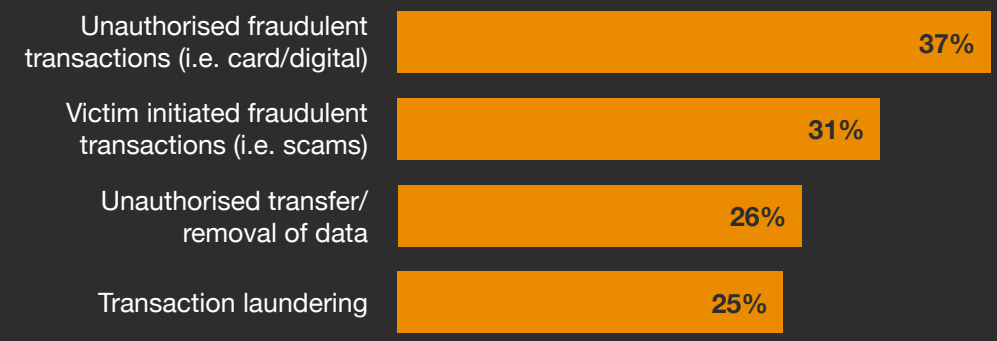
Over three quarters of organisations state platform fraud resulted from a fraudulent transfer to/from a platform

How platform frauds were executed

NET: Fraudulent access to platform

60%

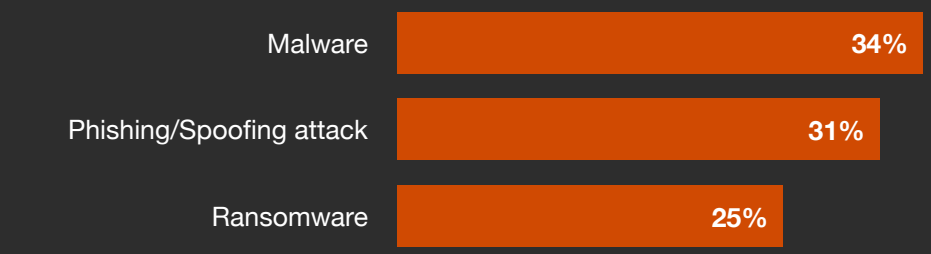
Fraudulent access to platforms is likely to be experienced across multiple platforms, in particular, **social media, knowledge, media sharing, services** or **goods platforms.**



NET: Fraudulent transfers to/from platform

76%

Of those experiencing fraud on their **Financial platforms**, this is most likely to be carried out by fraudulent transfers to/from a platform **(83%).**



NET: Fraudulent activity on the platform

60%

Of those experiencing fraud on their **Enterprise platforms**, this is most likely to be carried out by fraudulent activity on the platform **(71%).**

These types of fraud can take place across multiple entities including social media, knowledge, media sharing, services and goods platforms.

Scams account for about a third of platform fraud incidents – but strategies have evolved far past the well-known trickery of emails from an overseas prince. Some of **today's deceits are quite sophisticated and can even unfold over several months.**

And these frauds can be creative. For example, a prominent career platform recently became a breeding ground for scammers posing as financial experts[1]. Fraudsters courted "marks" by developing relationships and earning their victims' trust – eventually pulling a bait-and-switch with a fake financial-transaction platform. When the scheme was revealed, a staggering 32 million fake profiles were zapped from the site.

Enterprise platforms are most likely to be the site of malware, phishing, money laundering and ransomware incidents. Ransomware, in particular, has grown into an especially dangerous threat with the potential to inflict catastrophic damage. In one incident earlier in 2022, major auto industry players were hit by ransomware attacks – shutting down operations at a company's North American plants for a full week[2].

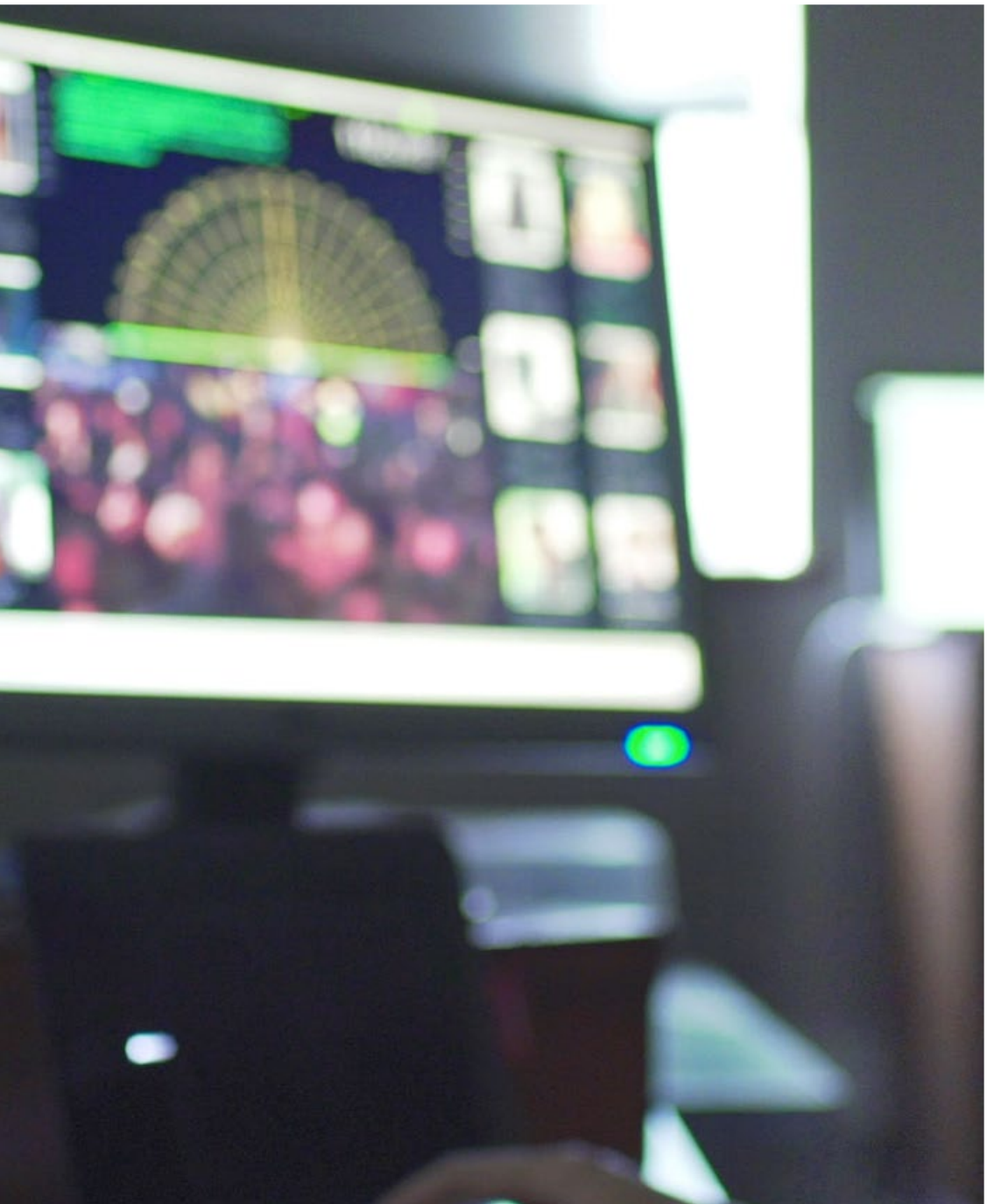
[1] Scott Zamost, CNBC, FBI says fraud on LinkedIn a 'significant threat' to platform and consumers. (17th June, 2022) Available at: www.cnbc.com/amp/2022/06/17/fbi-says-fraud-on-linkedin-a-significant-threat-to-platform-and-consumers.html

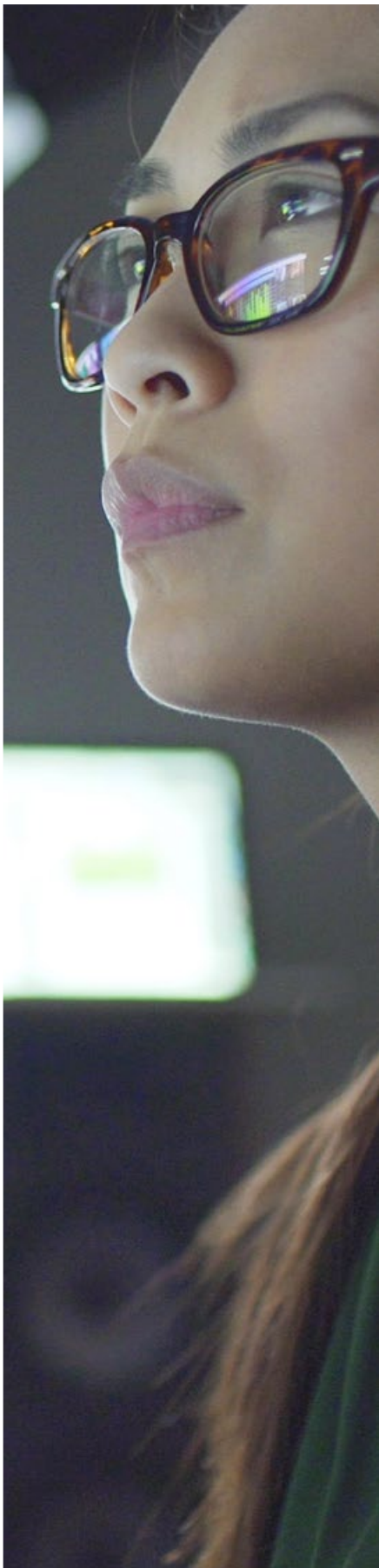
[2] Thomson Reuters, Japan's Bridgestone Reports ransomware attack at U.S. subsidiary (18th March, 2022) Available at: www.reuters.com/business/autos-transportation/japans-bridgestone-reports-ransomware-attack-us-subsidiary-2022-03-18/

Underestimating the threat

03

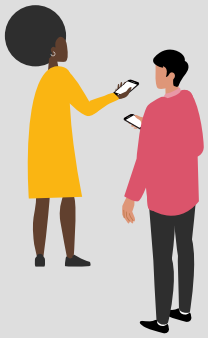
Well-established platform players have likely long been equipped with the proper security and controls to manage risk. But for newer entrants to the platform environment, there is dangerous potential for mushrooming risk. Perpetrators have become more sophisticated. The stakes are high. But still, our survey shows too many business leaders, both providers and users, aren't fully aware of their exposure.





91%

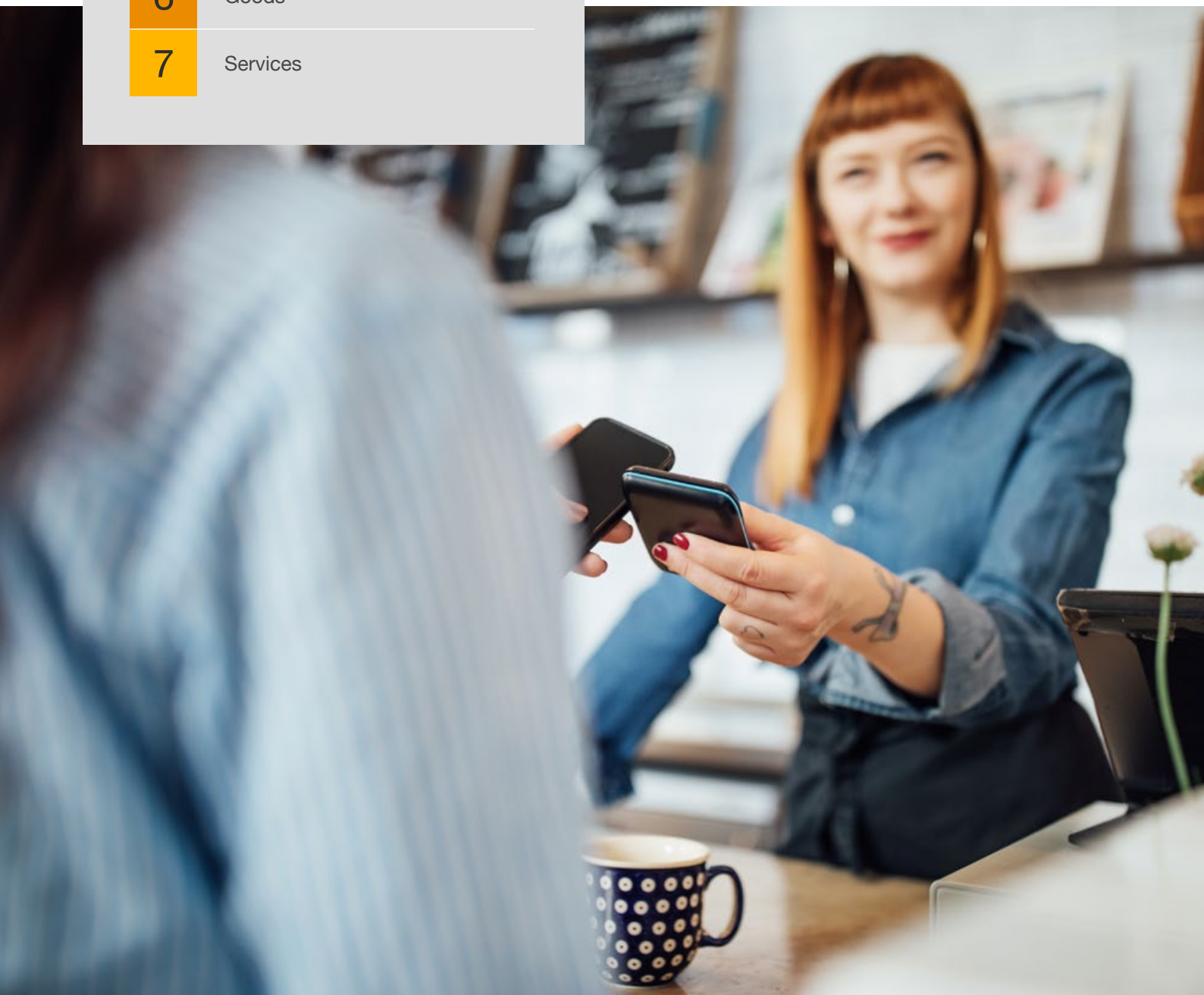
of fraud incidents in the past 24 months have been on one of these platforms:



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

Although platforms have emerged since the start of the pandemic as a major economic force, organisations don't necessarily view them as a discrete sector. Consequently, 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 for security is also transferred – except many platforms are not as well equipped as banks to identify, prevent and mitigate fraud. And transparency evaporates: In far too many instances, platforms do not provide their customers adequate visibility into how they manage consumer data – exposing all involved players to potential fraud.



Combatting platform fraudsters

04

Financial gain is the most common motive in platform fraud cases, at nearly 60% of all incidents. Almost half of all fraud cases take place on financial platforms – the most vulnerable model, particularly those involving funds transfers. But financial impact is just the beginning. Brand damage can be devastating. The undoing of customer loyalty and trust – catastrophic.

53% of perpetrators commit fraud for financial gain.

26% of organisations lost more than US$1m from platform fraud.

Over half of organisations state that platform fraud resulted in financial loss with over a quarter losing over $1 million as a result

Outcomes as a result of platform fraud

The data is undeniable: Platform fraud has opened a new frontier for fraud and economic crime. But with proper security and controls in place, organisations can protect themselves. An understanding of who the criminals 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.

Our survey reveals that nearly half of platform crimes are committed by external actors – a substantial uptick from 2020, when our GECS report indicated 41% of perpetrators were external. The boost is likely aligned with the explosive pandemic-era growth in platforms – and along with it, opportunities for malfeasance.

Main platform fraud perpetrators

23%
Collusion between internal and external actors

49%
External perpetrator

28%
Internal source

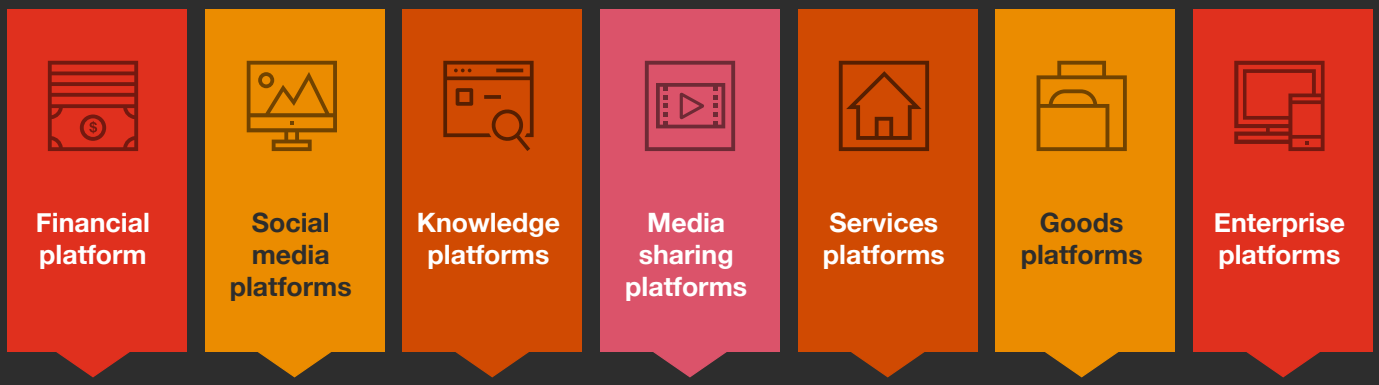
Organised crime has increased significantly since the coronavirus pandemic, which contributed to the rise in new platforms and created the opportunity for massive payoffs. Organised crime now accounts for 28% of incidents.

Who's leading the pack of external perpetrators? Hackers, who make up nearly half of all platform fraudsters. Organised crime is a new entrant to the top-three perpetrators of platform fraud, responsible for 28% of incidents, followed closely by customers at just over a quarter. Interestingly, customers led hackers by a tiny margin in 2020 (26% to 24%), followed by vendors at 19%.

It is notable that organised crime was of little consequence in platform fraud prior to the pandemic, when the opportunity for massive payoffs became a prime motivator. **Platform fraud has become a criminal enterprise – reinforcing the imperative for organisational resilience and the right tools to reduce your risk.**

However outcomes differ depending on types of platforms affected

Outcomes by type of platform fraud



Frauds occurring on these platforms are significantly more likely to result in…

Financial platform	Social media platforms	Knowledge platforms	Media sharing platforms	Services platforms	Goods platforms	Enterprise platforms
Financial losses (62%)	Lowered tone and control environment (28%)	Business / operational disruption / failure (42%)	Loss of new business opportunities (35%)	Financial losses (43%)	Lost new business opportunities (37%)	Business/ operational disruption/ Failure (39%)
		Regulatory action (34%)			Regulatory action (32%)	
		Increased incidents / more repeats (32%)			Increased incidents/ more repeats (31%)	

Identify, assess, execute

05

How can companies protect themselves on this new frontier – particularly given how quickly the platform threat environment is evolving?

Here are four key actions your business can take:

1 Elevate responsibility for platform risk management to a Chief Risk Officer

A C-suite level executive should be responsible for risk control policy and should provide effective challenge to the business. This is an imperative – a basic tenet of Risk 101: Organisational leaders must be accountable for guiding the risk management program – particularly when an emerging threat has the potential to upend your business. Platform fraud requires executive attention and an integrated, enterprise-wide response strategy with a focus on resilience as its foundation.

2 Stay vigilant for red flags

Only 37% of our respondents said they feel confident in their ability to respond effectively to platform fraud – a particularly unsettling statistic, given the threat level. And simply understanding the potential for criminal activity isn't the end game; risk leaders need to be proactive and design a meaningful strategy to identify, assess and execute a fraud response – because the consequences can be devastating.

In one notable fraud case, a major bank provided a payment platform for a handful of retailers that didn't have the infrastructure or capabilities to host their own transactions. The bank didn't sufficiently monitor its customer base, however, allowing a number of fraudsters to infiltrate – and when the damage was done, the bank was held responsible for its failure to identify red flags.

What are the warning signals? Red flags vary according to the type of platform. But knowing what to look for is the first step in protecting your perimeter. Each organisation, platform owners and even larger users, should have a list of specific red flags for their business. A few examples include:

Chargebacks

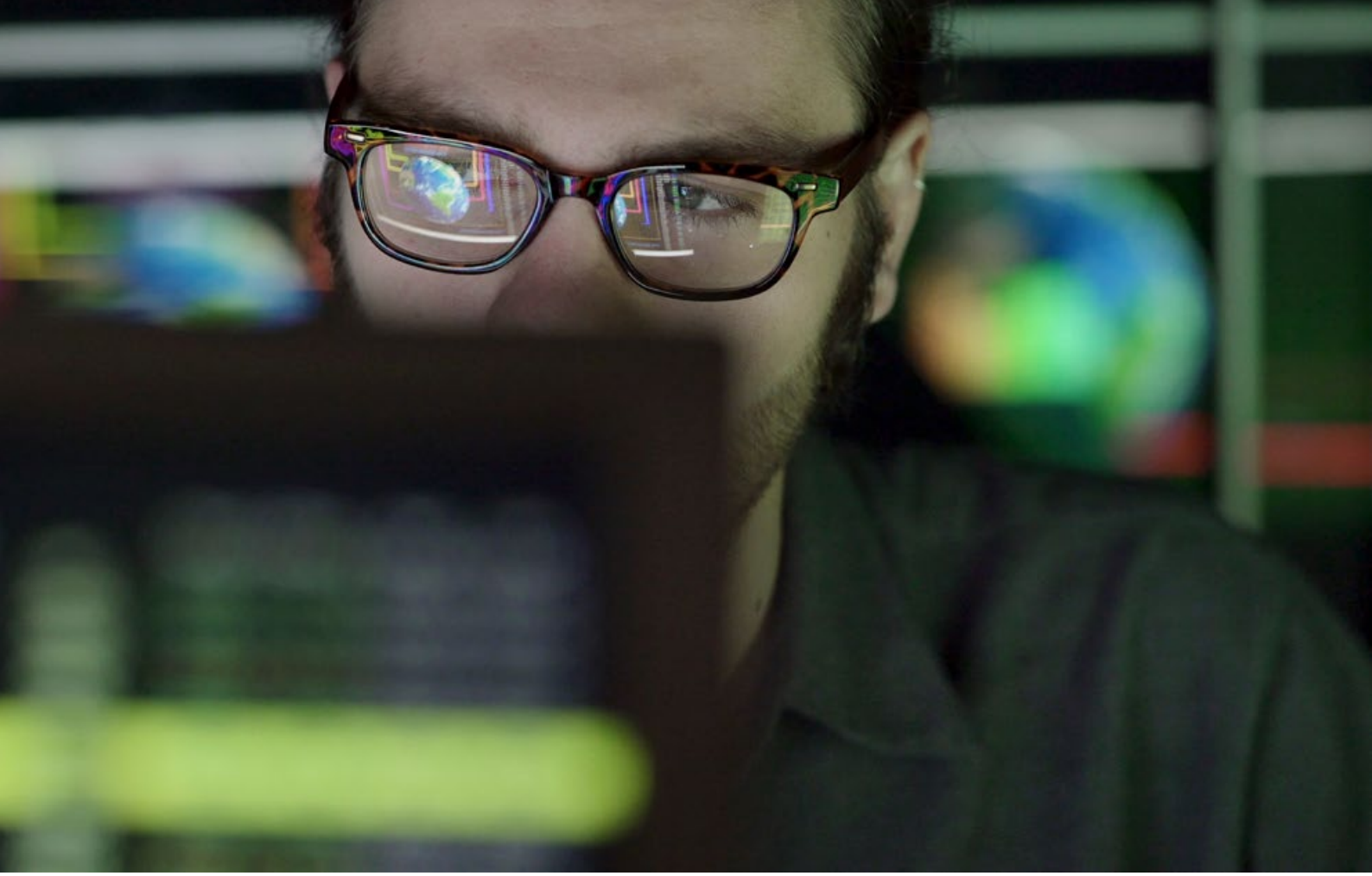
A rejection from the issuing bank for non-sufficient funds or a reservation voided or declined are the most common types of chargebacks. This can be tricky for platforms that engage with business travelers, for example, who may use multiple addresses in any given week. A monitoring program that identifies anomalies and alerts the company is key.

Bursts of activity

A spike in movement – whether rapid invoice generation or a notable increase in social media posts or other online activity – can signal a scheme in motion. Be aware of long periods of dormancy followed by these kinds of flare-ups.

Negative media coverage

If platforms are 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. Depending on the size and sophistication of your business and your level of engagement with platforms, social media monitoring is another important tool to keep you on top of what's happening in the market and alert to potential bad actors.



3 Measure, monitor, control

Establish controls to reduce your risk. Conduct a risk assessment to determine your exposure, and establish protocols for gaining visibility into platforms you work with. Your customers are your customers – and they trust you with their personal data.

Regardless of whether a major retail platform handles your financial transactions, your company name is on the receipt. Purpose-built transaction monitoring systems are necessary and effective 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

Know your environment and know your capacity for managing risk – particularly emerging risks, in addition to fraud, that aren't necessarily on the radar. Among them:

Sanctions evasion

Fraudsters are increasingly circumventing sanctions in certain jurisdictions in order 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)

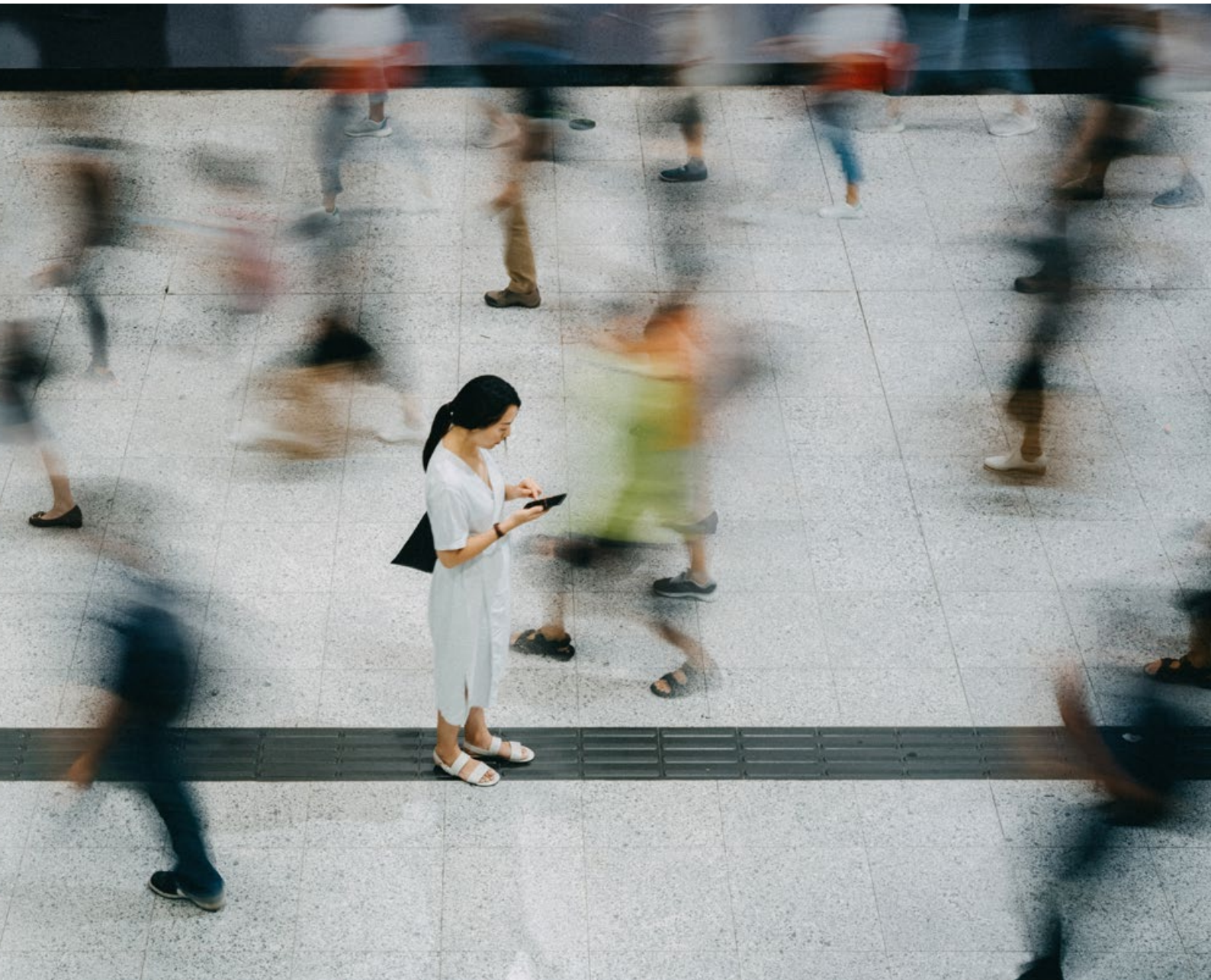
Under this broad umbrella encompassing environmental, social and governance issues, rising criminal threats include human trafficking and privacy invasion – by government entities, in some cases, as a cost of doing business.

A dangerous, growing risk

06

The sophistication and rapid proliferation of today's platform fraud perpetrators present a substantial risk. And although fraud incidents overall have remained somewhat steady for the past six years, platform fraud has emerged as the most aggressive threat of the era – particularly as the pandemic has accelerated digital transformation and sparked a sea change in how we conduct financial transactions.

The answer may lie in technology: Respondents to our 2022 survey reveal a number of 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 the survey

The aim of our two GECS reports was to provide a snapshot view of corporate perspectives toward fraud and financial/economic crime, its effect on business ethics and compliance programs, and to understand what types of fraud are most common. Snapshot 1 focused on risks associated with ESG and supply chain fraud, and Snapshot 2 focused on platform fraud.

1	**We surveyed organisations** from late 2021 through spring 2022
2	**2,300+** business leaders responded
3	**63%** of respondents are C-suite level
4	**69** countries are represented in our report
5	**6** languages are represented
6	**2** surveys were distributed

Contacts

Jeff Lavine
Global Financial Crimes Leader,
PwC US
jeff.lavine@pwc.com

Kristin Rivera
Global Forensics Leader, Partner,
PwC US
kristin.d.rivera@pwc.com

Ryan Murphy
US Forensics & Investigations Leader, Partner,
PwC US
ryan.d.murphy@pwc.com

Claire Reid
UK Forensics Services Leader, Partner,
PwC UK
claire.reid@pwc.com

Claudia Nestler
Germany Forensics Services Leader, Partner,
PwC Germany
claudia.nestler@pwc.com

Mark Rigby
Australia Forensics Services Leader, Partner,
PwC Australia
mark.rigby@pwc.com

Sirshar Qureshi
EMEA Forensics Co-Leader, Partner,
PwC Czech Republic
sirshar.qureshi@pwc.com

Stefan Heissner
EMEA Forensics Co-Leader, Partner,
PwC Germany
stefan.heissner@pwc.com

www.pwc.com/fraudsurvey