GBG

GLOBAL FRAUD REPORT

Burnt out and bombarded

Exposing the harsh realities of the impact of fraud on businesses and their teams.

APAC

2024

Fraud is always present.

But that's not to say it's standing still.

Having undergone its own industrialisation, fraud is a profit-making business machine and no organisation is safe from being a potential target. After all, criminals don't limit attacks to one business, industry or stop at national boundaries. Trends show fraud can spread rapidly across regions and industries, shape-shifting as it does so thanks to advances in technology.

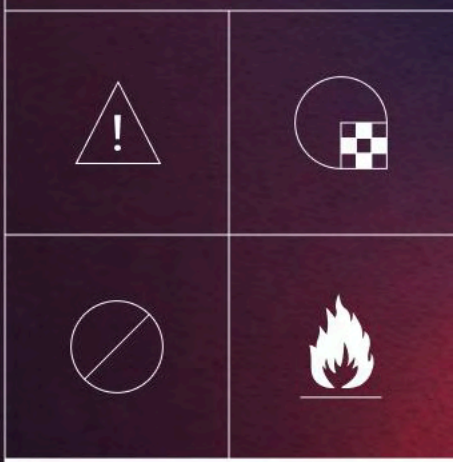
Since 2016, GBG IDology's market-leading annual fraud report has sought to gain a deeper understanding of the landscape US fraud prevention professionals are operating in. This year, GBG is expanding this to include the APAC and EMEA regions to deliver a global view into fraud trends and unique insights on local nuances.

This report is based on findings from a global survey of 1,200+ senior fraud prevention, risk and compliance professionals, with a focus on the experience of respondents in Australia, New Zealand, Malaysia, Indonesia, Thailand and the Philippines in the following industries: Banking, Ecommerce, Financial services (including Superannuation), FinTech (includes Payments and Remittances), Gaming & Wagering, Insurance, Lending and Telecommunications.

Carol Chris
General Manager, APAC
GBG

CHAPTER 1

Fraud Burnout



Anyone on the frontline in the fight against fraud will not only appreciate that the global fraud landscape is evolving, but that this is also impacting organisations' strategic direction.

Q. How do you perceive the evolving landscape of fraud and financial crime globally, and how does it impact your organisation's strategic direction?

	% of respondents
Fraud perceptions shift towards real-time monitoring and action	45%
Global fraud trends emphasise adaptability and quick responses	45%
Global fraud trends push for stricter compliance and oversight	43%
Focus on employee awareness shapes strategic training initiatives	42%
Evolving fraud landscape demands holistic risk management	41%

Of course, one of the main shifts fraud prevention professionals are experiencing is the rise of organised and widespread fraud.

Not only are almost all (97%) fraud prevention professionals we surveyed worried[1] about the trend towards more organised and widespread fraud, but almost 8 in 10 (77%) have seen a significant increase in sophistication by fraudsters in the last 12 months. Meanwhile, almost 2 in 5 (37%) say sophisticated fraud is currently proving more of a threat to their business.

% of respondents who have seen a significant increase in sophistication by fraudsters in the last 12 months

Banking **84%**

Financial services (including lending, insurance, fintech) **78%**

Gaming & Wagering **77%**

Telecommunications **67%**

The findings also confirm that advances in technology are facilitating the increasing sophistication of fraud tactics.

The highest percentages of fraud prevention professionals say they see Generative AI (35%), deepfakes (33%) and AI voice manipulation and replication (31%) as being the biggest trends in identity verification and fraud detection over the next 3-5 years. However, the findings also reveal that these fraudsters are wasting no time in putting these new technologies to immediate use as 31% of fraud prevention professionals surveyed state that AI voice manipulation and replication is the most prevalent fraud typology in their industry, while 28% say the same of deepfakes.

97%

are worried[1] about the trend towards more organised and widespread fraud

77%

have seen a significant increase in sophistication by fraudsters in the last 12 months

Q. Within your industry, how worried are you about the following types of fraud?

	 Banking	 Financial services (including lending, insurance, fintech)	 Gaming & Wagering	 Telecommunications
AI voice manipulation and replication	67%	76%	73%	71%
Deepfakes	71%	79%	76%	67%

When it comes to the evolution of GenAI in identity verification and financial fraud, fraud prevention professionals are also concerned about a range of fraud vectors.

The use of GenAI and machine learning in launching more complex attacks is also causing headaches for fraud prevention professionals in EMEA and the US.

Indeed, those we surveyed in the EMEA region are most likely to say they think generative AI (27%) and machine learning (27%) will be the biggest trends in identity verification over the next 3-5 years, while a quarter (25%) believe this will be AI voice manipulation and replication.

Meanwhile, over a quarter (27%) of US fraud prevention professionals believe GenAI is going to be the biggest trend in identity verification in the coming years and over 2 in 5 (44%) think that its use as a tool to create more convincing synthetic identities is the most threatening fraud vector.

Q. With the evolution of Generative AI in identity verification and financial fraud, what specific vector do you see being most threatening?

Fraud vector	% of respondents who believe this is most threatening
Generative AI as a tool to create more convincing synthetic identities	27%
Increased accuracy of fake ID documents generated by AI	26%
Generative AI's influence on phishing & smishing	26%
Use of generative AI to create deep fakes	21%

Top three biggest trends in identity verification and fraud detection for next 3-5 years by country

	APAC	EMEA	US
1	Generative AI (35%)	Generative AI (27%)	Generative AI (27%)
2	Deepfakes (33%)	Machine learning (27%)	Machine learning (13%)
3	AI Voice manipulation and replication (31%)	Submitting ID documents via mobile devices (27%)	More compliance and regulatory requirements (such as KYC, AML checks and transaction screening) (12%)

At the same time, fraud prevention professionals are also being plagued by myriad mobile-based fraud techniques.

Top 5 most prevalent mobile-based fraud techniques in APAC

SMS Interception	**42%**
Call forwarding	**41%**
Porting	**39%**
Recycling phone numbers	**39%**
SIM Swapping	**39%**

Of course, fraud prevention professionals aren't only concerned with sophisticated fraud and advancing tactics. In fact, opportunistic and convenient fraud remains a major issue, with almost two thirds (63%) saying this type of fraud is currently more of a threat to their business.

The findings paint a grim picture for those tasked with fending off numerous fraud attempts with an average[2] transactional value of $14.3k, with 1 in 9 (11%) saying that the average transactional value of attempted fraud attacks at their organisation is $35,000-$50,000.

Unsurprisingly, this heavy burden has been chipping away at the mental well-being of fraud prevention professionals, many of whom have also personally been a victim of fraud in the last 12 months (70%).

The fact is that fraud never sleeps, and neither do the ones trying to stop it.

We discovered that all (100%)[3] fraud prevention professionals surveyed are losing sleep over the risk fraud poses to their organisation, with respondents most likely to say verification of identity (46%) and insufficient resources (44%) keep them up at night.

Q. When thinking about the fraud risk at your organisation, what keeps you up at night?

	% of respondents
Verification of identity	46%
Insufficient resources	44%
Lack of regulations or controls	42%
Shifting tactics used by fraudsters	42%
Organisational silos between compliance, fraud and identity teams	39%
Industry silos	36%

Meanwhile, those we surveyed are experiencing a wide range of challenges including understanding the latest fraud trends (28%), lack of resource (28%) and identifying and stopping fraud at the point of onboarding (27%).

28%

say understanding the latest fraud trends is their biggest challenge

27%

say identifying and stopping fraud at the point of onboarding is their biggest challenge

27%

say keeping ahead of regulation is their biggest challenge

25%

say making accurate onboarding decisions is their biggest challenge

Our research provides a concerning insight into the minds of fraud prevention professionals. Racked with worry over advancing fraud tactics, facing numerous challenges and losing precious sleep, fraud prevention teams are suffering.

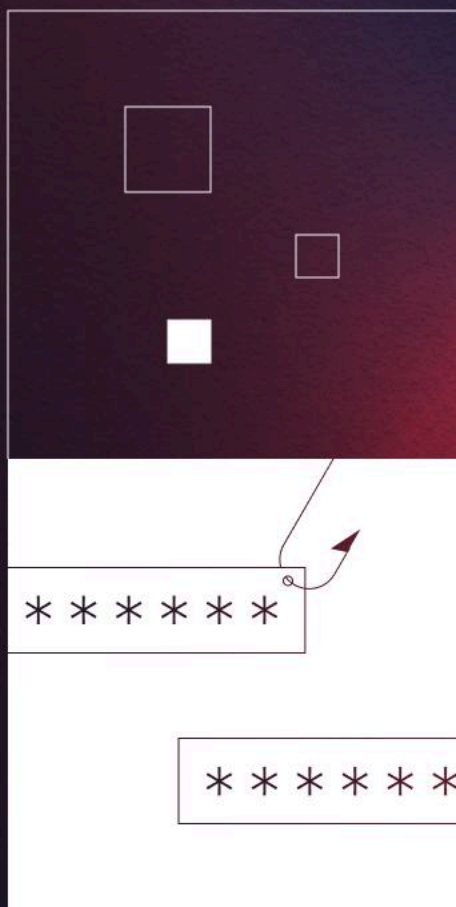
However, they aren't alone.

Notes:

1. 'Extremely worried', 'Very worried' and 'Somewhat worried' responses combined.
2. Mean: ($ excl. "I'm not sure")
3. Reverse of 'Nothing keeps me up at night'.

CHAPTER 2

Fraud is everyone's problem

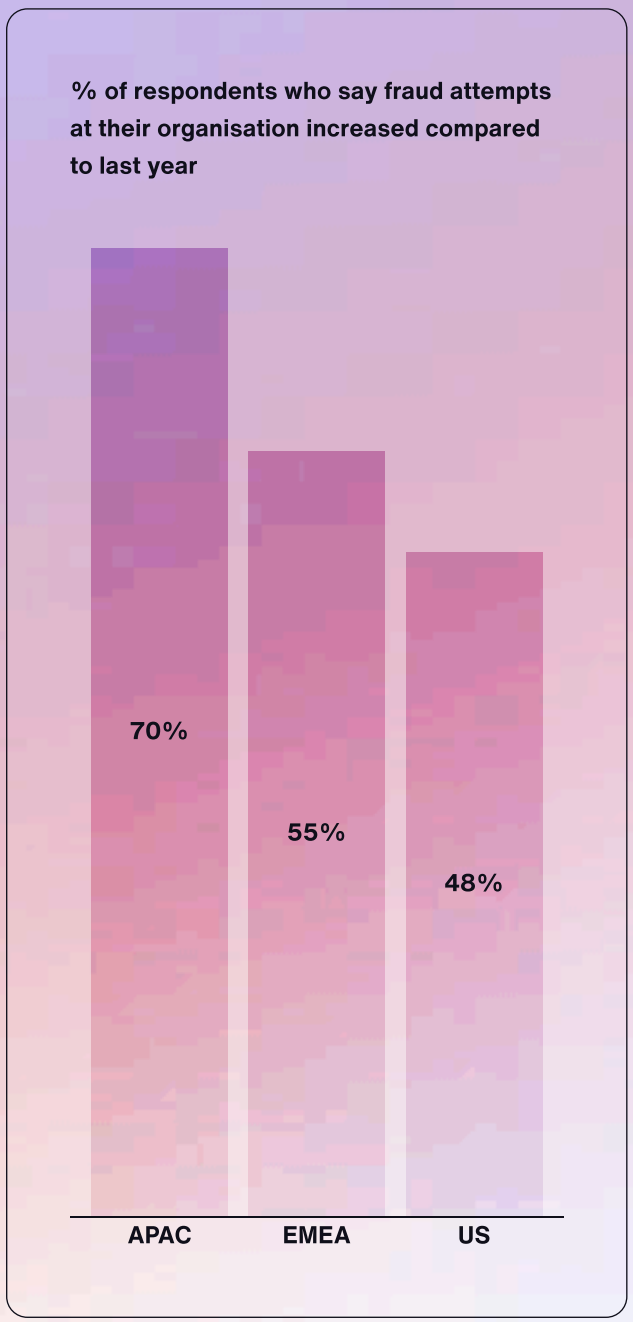


Sleep-deprived fraud prevention professionals have been left feeling isolated by fraud, with almost 2 in 5 (39%) saying organisational silos between compliance, fraud and identity teams have been keeping them up at night, while almost 2 in 5 (36%) are losing sleep over industry silos.

However, findings from our global study show that they are far from alone in the fight against fraud.

In fact, fraud is a global, cross-industry problem that's impacting fraud prevention professionals all over the world. And it's on the rise.

This is especially the case in the APAC region where 7 in 10 (70%) say fraud attempts at their organisation increased compared to last year, while 55% of those in EMEA and 48% of those in the US say the same.



In the APAC region, respondents report that they have seen an increase in various types of fraud in their industry.

We discovered:

41%

have seen an increase in impersonation of digital presence (spoofed websites, social media, emails etc.)

40%

have seen an increase in account takeover fraud

39%

have seen an increase in bonus or promotion abuse

39%

have seen an increase in money laundering and money mules

Q. Within your industry, have you seen an increase or decrease in the following types of fraud?

	Banking	Financial services (including lending, insurance, fintech)	Gaming & Wagering	Telecommunications
Account takeover	39%	44%	43%	40%
Bonus or Promotion Abuse	37%	42%	40%	44%
Identity Theft	39%	35%	43%	50%
Credit card/debit card/prepaid card fraud	42%	43%	34%	54%
First-party fraud	32%	42%	41%	27%
Money-laundering and money mules	42%	40%	41%	27%
Internal fraud	34%	40%	49%	42%
Third-party fraud	35%	33%	41%	29%
Impersonation of digital presence (spoofed websites, social media, emails, etc)	46%	40%	39%	37%
Mobile device attacks (malware, hacking, etc.)	37%	45%	49%	44%
Deepfakes	47%	51%	59%	46%
AI voice manipulation and replication	37%	47%	57%	40%
Social engineering	30%	45%	44%	38%

Given the vast range of tactics being deployed across today's fraud landscape, it's no wonder fraud prevention professionals across the globe feel that identity verification and fraud detection has become more complicated and complex for businesses in the last three years.

Unsurprisingly, high percentages of fraud prevention professionals surveyed in the APAC region also said they are worried about various types of fraud.

% of fraud prevention professionals who think identity verification has become more complicated and complex for businesses in the last 3 years

APAC	**67%**
EMEA	**62%**
US	**54%**

Country most worried about various types of fraud vs APAC region overall

(Q. Within your industry, how worried[1] are you about the following types of fraud?)

Type of fraud	% of respondents who are worried[1] about this type of fraud in the APAC region	Country with highest % of respondents worried about this type of fraud
Mobile device attacks (malware, hacking, etc.)	77%	Malaysia (87%)
Impersonation of digital presence (spoofed websites, social media, emails, etc)	76%	Australia (80%)
Deepfakes	75%	Malaysia (83%)
Account takeover	74%	Thailand (81%)
Credit card/debit card/prepaid card fraud	74%	Malaysia (88%)
First-party fraud	73%	Australia (79%) / Thailand (79%)
Money-laundering and money mules	73%	Thailand (79%)
Internal fraud	73%	Australia (80%)
Identity Theft	72%	Malaysia (79%)
AI voice manipulation and replication	72%	Malaysia (85%)
Social engineering	71%	Australia (74%)
Bonus or Promotion Abuse	70%	Australia (77%)
Third-party fraud	70%	Australia (77%)

The findings show that fraud prevention professionals in the APAC region have a similar level of concern about certain types of fraud as those in EMEA and the US.

For example, 73% of respondents in EMEA say they are worried[1] about synthetic identity fraud, 72% are worried[1] about bonus/promotion abuse, 71% are worried about deepfakes and 67% say they are worried[1] about account opening fraud.

Meanwhile, 69% of US fraud prevention professionals say they are worried[1] about synthetic fraud. However, fewer US respondents say that they are worried about bonus/promotion abuse fraud (55%).

The study shows that fraud prevention teams have every right to be worried, as data breaches have had a widespread negative impact on business in all regions in the past 12 months.

Meanwhile, every industry in the APAC region has been impacted by data breaches in one or more ways.

% of businesses that have faced major financial and/or reputational consequences as a result of a data breach in the past 12 months

APAC	**68%**
EMEA	**65%**
US	**37%**

Q. What impact have recent, large scale data breaches had on fraud within your industry in the last 12 months?

% of respondents who have been impacted in this way as a result of data breaches

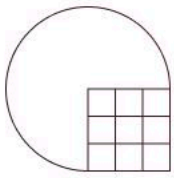
	Banking	Financial services (including lending, insurance, fintech)	Gaming & Wagering	Telecommunications
Increase in confirmed fraud	46%	41%	46%	44%
Increase in synthetic identity fraud /identity theft	39%	44%	49%	33%
Increase in fraud risk	45%	37%	39%	38%
Increase in customer friction	44%	34%	33%	33%
Increase in compliance and regulation	35%	39%	31%	44%
Increase in risk-averse business practices	38%	39%	34%	31%
No impact	2%	0%	0%	0%

Notes:

1. 'Extremely worried', 'Very worried' and 'Somewhat worried' responses combined.

CHAPTER 3

Opening the door to fraudsters



While it is concerning that new technologies including AI are enabling fraudsters to evolve their tactics, there is also ample opportunity for fraud prevention and compliance divisions to leverage onboarding technology to fend off attacks.

And yet, almost a fifth (19%) of fraud prevention professionals are vulnerable to attacks because they don't have the right technology in place today to fight the advanced criminal networks that combine cybercrime, fraud, identity theft and money-laundering to execute end-to-end fraud.

Q. Do you feel you have the right technology in place today to fight the advanced criminal networks that combine cybercrime, fraud, identity theft and money-laundering to execute end-to-end fraud?

	% of respondents in...					
	Australia	**New Zealand**	**Malaysia**	**Indonesia**	**Thailand**	**Philippines**
Yes	78%	93%	58%	77%	73%	82%
No	21%	5%	37%	17%	23%	18%
Unsure	1%	2%	6%	6%	4%	0%

The study also reveals that many fraud prevention professionals are still letting fraudsters get their foot in the door, choosing instead to apprehend them once they have already infiltrated their business. Much like their counterparts in the EMEA region (35%), only 36% are investing the most spend and resource for fraud detection and prevention at the account opening stage. Meanwhile, almost two thirds (64%)[1] are choosing to prioritise ongoing transaction monitoring and catching fraudsters at the payment or withdrawal stage.

On top of this, just over a fifth (21%) of fraud prevention professionals surveyed say they are not using any risk signals at the top of their funnel.

Unsurprisingly, over a fifth (22%) say they find it extremely difficult to identify fraudsters at the point of onboarding, which rises to just over 3 in 10 (31%) respondents in Malaysia and almost 3 in 10 (29%) of those we surveyed in Australia.

In fact, over a quarter (27%) of fraud prevention professionals in the APAC region say identifying and stopping fraud at the point of onboarding is one of the biggest challenges they face in their job.

The findings certainly seem to suggest that despite the obvious need for businesses to differentiate between good and bad customers, many are reluctant to stop fraudsters in their tracks at the beginning of the customer journey.

% of respondents not using any risk signals at the top of their funnel

APAC	**21%**
EMEA	**30%**
US	**18%**

It's likely that the reason for this is that fraud prevention professionals are anxious not to put good customers off with excessive verification processes.

Indeed, all fraud prevention professionals surveyed believe it's important[2] to consumers that the process of opening a new account online is quick (100%) and easy (100%).

It's no wonder that almost all (95%) those we surveyed are worried[3] about the added friction of robust fraud checks impacting onboarding for good customers.

This is the case across all industries.

Q. Are you worried about the added friction of robust fraud checks impacting onboarding for good customers?

% of respondents who are worried[3] about the added friction of robust fraud checks impacting onboarding for good customers

Banking **93%**

Financial services (including lending, insurance, fintech) **97%**

Gaming & Wagering **94%**

Telecommunications **98%**

However, 100% of the fraud prevention professionals we surveyed also believe it's important[2] to consumers that the process of opening an account online is secure.

In essence, fraud prevention professionals have been set the complex task of delivering identity verification solutions that are vigorous enough to withstand a barrage of fraud attacks while remaining both quick, easy and secure without adding friction that impacts the onboarding of good customers.

It's no mean feat.

The question is, is it possible?

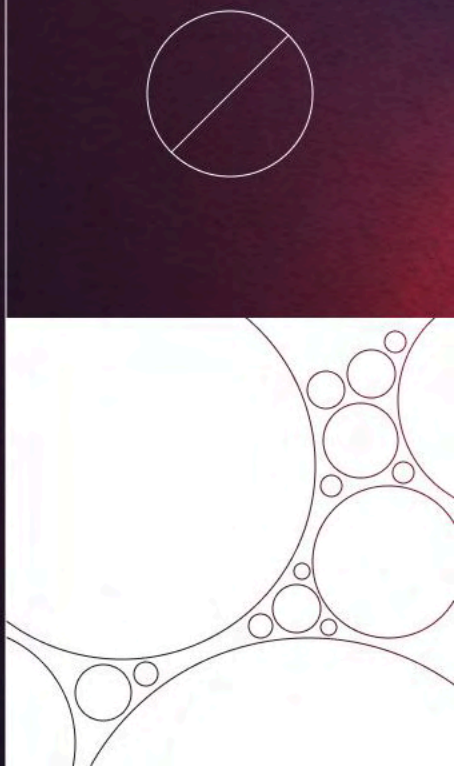
Notes:

1. '2' and '3' responses combined.
2. 'Extremely important', 'Very important' and 'Moderately important' responses combined.
3. 'Extremely worried', 'Very worried' and 'Somewhat worried' responses combined.

CHAPTER 4

Why wait?

The contradictions holding back fraud prevention professionals



If fraud is everyone's problem, it seems only fair that the solution is everyone's responsibility.

Cross-sector collaboration on a global scale may well be the silver bullet fraud prevention and compliance divisions have been looking for to tackle fraud. Not only does it enable businesses to apply friction at the point of onboarding where necessary, it also allows them to identify good and great customers while providing them with an exceptional user experience.

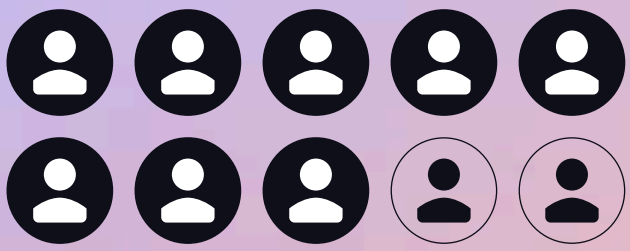
Most fraud prevention professionals we surveyed agree. In fact, 81% think cross-sector identity intelligence sharing and collaboration can be a strategic differentiator in beating fraud.

However, our research reveals that while businesses see the benefit of working alongside others to combat fraud, and many (81%) are already part of an identity intelligence consortium/network that enables this collaboration, in practice their efforts are lacking.

In fact, less than half of fraud prevention professionals are taking various steps to combat fraud including actively participating in industry forums and working groups for knowledge exchange (47%), investing in tech solutions facilitating secure data exchange (46%) and establishing partnerships with law enforcement agencies for information sharing (46%).

At the same time, few organisations are committed to assessing the effectiveness of their current fraud prevention and detection efforts by regularly reviewing fraud incidents and trends for insights (42%), analysing false positives and detection rates (41%), and tracking response time to fraudulent activities (38%).

It's no wonder that so many fraud prevention professionals admit that their organisations aren't pulling their weight in the fight against fraud.



81% think cross-sector identity intelligence sharing and collaboration can be a strategic differentiator in beating fraud

% of respondents who think cross-sector identity intelligence sharing and collaboration can be a strategic differentiator in beating fraud

Australia	**78%**
New Zealand	**97%**
Malaysia	**67%**
Indonesia	**73%**
Thailand	**77%**
Philippines	**88%**

% of respondents whose organisation is part of an identity intelligence consortium/ network which enables cross-sector intelligence to be shared to combat fraud

Australia	**79%**
New Zealand	**94%**
Malaysia	**58%**
Indonesia	**75%**
Thailand	**77%**
Philippines	**92%**

81%

agree[1] that organisations are letting down their customers by not prioritising cross-sector collaboration to combat fraud

82%

agree[1] that organisations aren't doing enough to collaborate with other industries and organisations to help combat fraud

83%

agree[1] that organisations are too worried about maintaining a competitive advantage to participate in cross-sector collaboration to combat fraud

On top of this, almost 4 in 5 (79%) agree[1] that governments around the world are not doing enough to support cross-sector collaboration to combat fraud.

Furthermore, just over a fifth (21%) of fraud prevention professionals say they don't feel governments around the world are collaborating to put strategies in place to fight international fraud, which rises to almost 2 in 5 (38%) of those in Malaysia. Meanwhile, almost a quarter (23%) don't feel like local governments are doing enough to help organisations fight fraud.

The research shows that on the whole, fraud prevention professionals are afraid to commit to cross-sector collaboration because they are worried[3] about sharing data with companies for competitive or data privacy reasons (97%).

Q. What do you think the government should be doing to help fight fraud?

	% of respondents[2]
Setting clear standards on fraud prevention requirements	58%
Supporting organisations with risk of data breaches	51%
Mandating cross-sector data and intelligence sharing	44%
Enforcing regulation	38%
Other	1%

% of respondents who are worried about sharing data with companies for competitive or data privacy reasons

	Australia	**New Zealand**	**Malaysia**	**Indonesia**	**Thailand**	**Philippines**
Extremely worried	37%	52%	29%	23%	21%	51%
Very worried	37%	26%	25%	37%	62%	33%
Somewhat worried	24%	18%	37%	35%	17%	14%

However, there is no more time for hesitation.

Businesses must take action against fraud now with readily available tools that will empower them to take a stand against even the most sophisticated fraudsters.

Notes:

1. Strongly agree' and 'Agree' responses combined.
2. Respondents who don't feel like the local government is doing enough to help organisations fight fraud (23%).
3. 'Extremely worried', 'Very worried' and 'Somewhat worried' responses combined.

CHAPTER 5

Building trust in digital identities

If there's one thing our research has revealed, it's that it's time for things to change.

Fraud, risk and compliance divisions are being pushed to the brink and suffering under the weight of their responsibility to protect organisations against an onslaught of increasingly sophisticated fraud attacks.

However, this issue is not confined to specific industries or specific regions.

The proliferation of fraud is a global problem that requires a global solution. It is therefore time for organisations in all industries across the world to set aside their misgivings on identity and financial fraud intelligence sharing and come together in a united front against fraud.

The concept of cross-sector identity intelligence sharing has already gained momentum as 81% of respondents surveyed in the APAC region are already part of a network. Now, companies are increasingly working together to achieve a new common objective: building trust in digital identities.

Available to businesses across the APAC region, GBG's identity verification and fraud prevention solutions can help to maximize your organization's defences against evolving fraud typologies while still allowing you to provide a frictionless customer experience. Our application fraud solutions help to reduce fraud loss at the point of onboarding by leveraging user data enrichment for fraud risk assessment, while our Digital Risk Management & Intelligence Platform enables fraud risk detection across the entire customer journey.

Businesses in Australia and New Zealand can also benefit from GBG Trust: Alert which allows businesses to detect fraud during onboarding using unrivalled proprietary analytics and intelligence derived from millions of cross-industry identity verifications.

To find out more about how GBG can help you to detect and prevent fraud, visit: https://www.gbgplc.com/apac

Methodology

GBG partnered with research consultants Censuswide to conduct this study in the APAC and European regions. The findings in this report are based on the following surveys:

APAC

Censuswide surveyed 520 CXOs, VPs, directors and managers in risk and fraud, operations and compliance roles between May 16 and 24 2024 in the following:

- **Sectors:** Financial services (including superannuation), insurance, fintech (including payments and remittances), banking, lending, telecoms, eCommerce, gaming and wagering
- **Company sizes (revenue):** <£50m / £50-100m / £100- 500m / £500m- £1bn / >£1bn
- **Countries:** Australia (213), New Zealand (100), Malaysia (52), Indonesia (52), Thailand (52), Philippines (51)

Europe

Censuswide surveyed 407 CXOs, VPs, directors and managers in risk and fraud, operations and compliance roles between April 26 and May 08 2024 in the following:

- **Sectors:** Financial services, fintech, banking, retail, gaming and crypto
- **Company sizes (revenue):** <£50m / £50-100m / £100- 500m / £500m- £1bn / >£1bn
- **Countries:** UK (255), France (50), Germany (52), Spain (50)

Censuswide abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Censuswide is also a member of the British Polling Council.

United States

GBG partnered with Qualtrics to conduct this study in the United States. Qualtrics surveyed 269 VPs, directors, managers and analysts in risk and fraud, compliance, operations and product roles between April 28 and June 17 2024 in the following:

- **Sectors:** Financial services, lending, insurance, healthcare, travel, hospitality, gaming and eCommerce
- **Company Size (revenue):** <$1m / $1-5m / $1-10m / $1-10m / $10-25m / $25-50m / $50-100m / $100-500m / $500m-1bn / $1-10bn / >£10bn
- **Countries:** United States

GBG