GBG

GLOBAL FRAUD REPORT

Burnt out and bombarded

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

Europe

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 machine and no organisation or individual 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, our market-leading annual fraud report has sought to gain a deeper understanding of the landscape that US fraud prevention professionals are operating in. This year, we are expanding this research to include Europe and Asia Pacific (APAC) regions in order to deliver a global view of current fraud trends with unique insights on local nuances.

This report is based on findings from a survey of 1,200+ senior fraud prevention, risk and compliance professionals, with a focus on the experience of respondents in the UK, Germany, Spain and France in the following industries: Banking, Crypto, Financial services, FinTech, Gaming and Retail.

Laura Barrowcliff
Head of Trust
GBG

CHAPTER 1

Fraud Burnout

It will come as no surprise to anyone tasked with protecting their business against a rising number of fraud attacks, that tactics old and new are employed by savvy fraudsters on an increasingly industrial scale.

Not only are almost all (96%) of fraud prevention professionals we surveyed worried[1] about the industrialisation of fraud, but almost 4 in 5 (79%) have seen a significant increase in the sophistication of fraud attempts in the past year. Meanwhile, almost a third (32%) say sophisticated fraud is currently proving more of a threat to their business.

Evolving technology is playing straight into the hands of fraudsters, with criminals now exploiting AI and machine learning to launch their attacks. Not only is the standard of fake and synthetic identities already at an all-time high thanks to emerging technology, but developments in this space are set to cause headaches for fraud prevention professionals for the foreseeable future.

Those we surveyed expect generative artificial intelligence (GenAI) (27%) and machine learning (27%) to be the biggest trends in identity verification and fraud over the next three to five years. Those who believe GenAI will be a major trend are most likely to say they see the increased accuracy of fake ID documents generated by AI (30%), GenAI's influence on phishing and smishing and the use of GenAI to create deepfakes (24%) as being the most threatening fraud vectors.

GenAI is also on the radar of US fraud prevention professionals. According to findings from our US survey, over a quarter (27%) of respondents believe GenAI is going to be the biggest trend in identity verification in the next 3-5 years. However, US respondents are twice as likely as those in Europe to think GenAI, used as a tool to create more convincing synthetic identities, is the most threatening fraud vector (44% vs 22%).

Fraud prevention professionals in the APAC region are more likely to say that GenAI (35%) will be the biggest trend in identity verification and fraud detection over the next three to five years.

96%

are worried[1] about the industrialisation of fraud

79%

have seen a significant increase in the sophistication of fraud attempts in the past 12 months

GenAI - Generative AI poses a threat to businesses as it allows fraudsters to easily fabricate realistic and hard-to-detect fake identities and documentation that can be used to carry out fraudulent activities.

Phishing – This common fraud uses scam emails containing links to websites that may contain malware – software designed to disrupt or gain unauthorised access to a computer system – or may be designed to trick recipients into revealing sensitive information or transferring money.

Smishing – Similar to phishing, smishing (SMS phishing) attacks are a form of social engineering carried out over text message, encouraging recipients to follow links to malicious websites, reveal sensitive information or transfer money.

44%

of US fraud prevention professionals believe GenAI used to create convincing synthetic identities is their biggest concern

22%

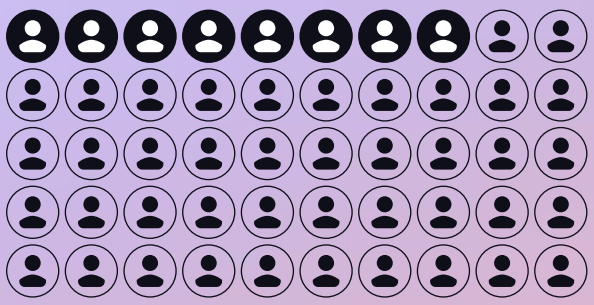
of European fraud prevention professionals believe GenAI used to create convincing synthetic identities is their biggest concern

27%

of APAC fraud prevention professionals believe GenAI used to create convincing synthetic identities is their biggest concern

Of course, fraud prevention professionals aren't only concerned about the industrialisation of fraud and evolving tactics. Opportunistic and convenient fraud attacks continue to plague their day-to-day lives with almost 7 in 10 (68%) saying this type of fraud is currently more of a threat to their business.

The business impact of fraud is well documented. According to our research, fraud prevention professionals are battling numerous fraud attempts with an average[2] transactional value of £18.2k, with 1 in 6 (16%) saying that the average transactional value of attempted fraud attacks at their organisation is £35-50k. In addition to this, we must also consider the reputational damage businesses incur having fallen victim to fraud and data breaches.



16% **of fraud professionals report average attempted fraud at £35-50k**

But what about the human cost of fraud? How has facing new and sophisticated fraud attacks, as well as continuous opportunistic attacks, day in and day out impacted fraud prevention professionals? Our findings show that living under the constant threat of fraud, which in the UK constitutes a massive 40% of all crime, has taken a worrying toll on the mental well-being of fraud prevention and compliance professionals, many of whom have also personally been a victim of fraud in the last 12 months (75%).

We discovered three in four (75%) fraud prevention professionals surveyed have experienced burnout in their job due to the rising levels of fraud.

75% **of fraud professionals have experienced burnout in their job due to the rising levels of fraud**

And it's no wonder given the risk fraud poses is keeping almost everyone (99%)[3] we surveyed up at night, with respondents most likely to be losing sleep over lack of regulations or controls (39%), verification of identity (39%) and shifting tactics used by fraudsters (37%).

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

	% of respondents
Lack of regulations or controls	39%
Verification of identity	39%
Shifting tactics used by fraudsters	37%
Industry silos	35%
Organisational silos between compliance, fraud and identity teams	33%
Insufficient resources	33%

The stark reality for many Heads of Fraud is that they are accountable when organisations succumb to fraud attacks. At the same time, recent reports have shown that organisations are axing risk management teams as they are perceived to be a blocker on transformation strategies. This is despite the immense pressure to protect organisations against fraud, which is set to become even more extreme in the UK when plans for authorised push payment (APP) fraud reimbursements come into effect this October. Both flawed and highly controversial, these new regulations stipulate that banks and payment companies must reimburse individual fraud victims to the tune of up to £415k; a sum that could easily force many smaller fintech companies out of business.

In short, the stakes for fraud prevention professionals have never been higher and they are suffering as a result.

However, they aren't alone.

Notes:

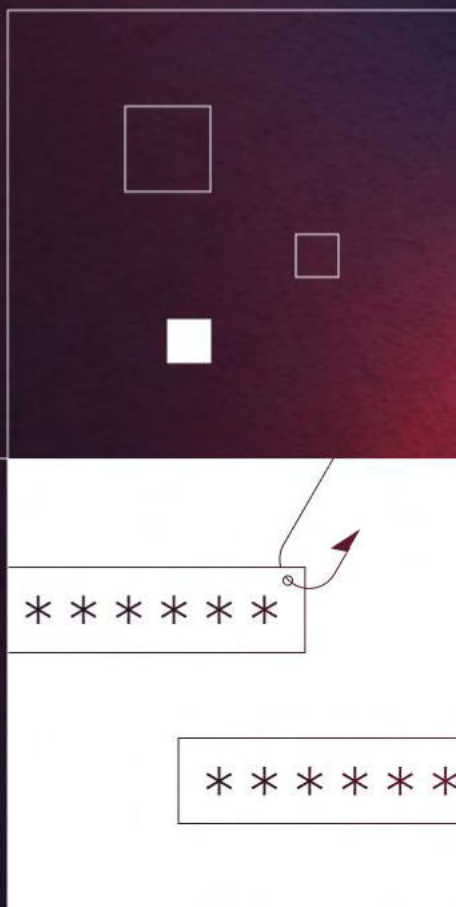
1. 'Extremely worried', 'Very worried' and 'Somewhat worried' responses combined.
2. Mean average.
3. Reverse of 'Nothing keeps me up at night'.

CHAPTER 2

Fraud is everyone's problem

"Research we've conducted at Datos Insights into Generative AI aligns with the growing concern around the technology's potential impact on fraud. These findings underscore the importance of understanding the intricate ways in which AI as a whole can be utilised in fraud perpetration and deterrence."

Becki LaPorte
Strategic Advisor, Datos Insights



Burnt out fraud prevention professionals have been left feeling sleep-deprived, fearful, and worried about a range of different and increasingly troublesome fraud vectors.

73%

are worried[1] about synthetic identity fraud

72%

are worried[1] about bonus or promotion abuse

71%

are worried[1] about deepfakes

67%

are worried[1] about account opening fraud

Fraud prevention professionals are feeling isolated, with industry silos keeping over a third (35%) up at night, while a third (33%) are losing sleep over organisational silos between compliance, fraud and identity teams. While fraud prevention, risk and compliance professionals have unique challenges, however, they aren't alone in their concerns.

Our research shows fraud is a global and cross-sector challenge confronting fraud professionals across Europe, APAC and the US.

Over 4 in 5 (82%) of fraud prevention professionals surveyed in Europe say their organisation experienced known or suspected fraud attempts in the last 12 months.

% of respondents in Europe who say their organisation experienced known or suspected fraud attempts in the last 12 months

UK	78%
France	92%
Germany	79%
Spain	92%

Over half (55%) of respondents in Europe say the number of fraud attempts at their organisation increased in the last 12 months; a shift also felt by fraud prevention professionals in the US and APAC regions.

At the same time, fraud prevention professionals in every industry in Europe have seen an increase in various types of fraud to some extent.

% of respondents who say fraud attempts at their organisation increased compared to last year

Europe	55%
US	48%
APAC	70%

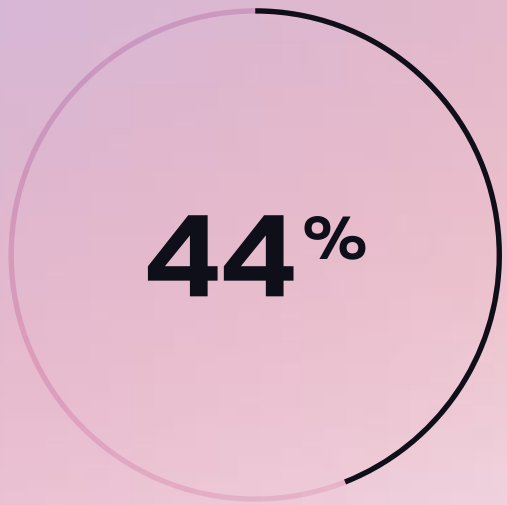
Q. Within your industry, have you seen an increase or decrease in the following types of fraud?

	% of respondents who have seen an increase in this type of fraud					
	Banking	**Crypto**	**Financial services**	**Fintech (inc Payments)**	**Gaming**	**Retail**
Synthetic identity fraud	36%	43%	37%	62%	43%	43%
Bonus abuse / Promotion abuse	42%	35%	44%	42%	48%	37%
Deepfakes	42%	39%	34%	32%	46%	43%
Account opening fraud	34%	36%	40%	42%	46%	33%

The research highlights that synthetic identity fraud is a growing concern, particularly within the Fintech industry.

Fraud prevention professionals in the US are also plagued by this issue. Synthetic identity fraud is the fastest-growing financial crime, with various estimates predicting that this form of fraud will result in losses of $2.42bn dollars in unsecured credit products and as much as $6bn in total losses to the banking sector.

With that in mind, it's unsurprising that 54% of US respondents say the identity market has become more complicated and complex over the past three years.



of US fraud prevention professionals believe GenAI used to create convincing synthetic identities is their biggest concern

The findings also reveal that data breaches have had a widespread negative impact on businesses across all regions in the past 12 months.

Meanwhile, every industry in Europe 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

Europe	**65%**
APAC	**68%**
US	**37%**

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

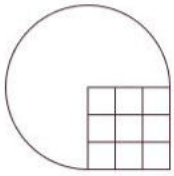
	% of respondents who have been impacted in this way as a result of data breaches					
	Banking	**Crypto**	**Financial services**	**Fintech (inc Payments)**	**Gaming**	**Retail**
Increase in confirmed fraud	32%	37%	42%	28%	41%	49%
Increase in risk-averse business practices	39%	52%	35%	32%	29%	31%
Increase in customer friction	36%	36%	37%	38%	38%	29%
Increase in fraud risk	40%	31%	44%	30%	33%	29%
Increase in synthetic identity fraud	32%	28%	31%	38%	38%	47%
Increase in compliance and regulation	38%	31%	40%	38%	30%	22%
No impact	3%	0%	0%	2%	0%	4%

CHAPTER 3

Opening the door to fraudsters

"Synthetic identity fraud is the fastest-growing financial crime, costing business billions of dollars in fraud losses, and every year the scam continues to grow."

Brett Johnson
Ex-synthetic identity fraudster



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.

Our research reveals that many fraud prevention professionals are still leaving the door to their business open to fraudsters, however, preferring to catch them mid-journey rather than at the onboarding stage.

Only 35% are investing the most spend and resource for fraud detection and prevention at the account opening stage, while almost two thirds (65%) are choosing to prioritise ongoing transaction monitoring to catch fraudsters at the payment or withdrawal stage[1]. A significant minority (30%) are not using any fraud risk signals at the start of their onboarding journey.

Unsurprisingly, 31% say they find it extremely difficult to identify fraudsters at the point of onboarding.

Identifying and stopping fraud at the point of onboarding (24%) is cited as one of the top three challenges fraud prevention professionals experience in their job, along with knowing the best tools to use (25%) and creating tailored customer experiences (24%).

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

Europe	**31%**
APAC	**21%**
US	**18%**

It appears that despite the need for businesses to differentiate between good and bad customers, something is clearly holding businesses back from deterring fraudsters at the beginning of the customer journey.

Our findings reveal that fraud prevention professionals are desperate not to put good customers off with disruptive identity 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 then that almost all (97%) of 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?

Industry	% of respondents who have been impacted in this way as a result of data breaches
Banking	97%
Crypto	99%
Financial services	94%
FinTech (inc payments)	98%
Gaming	98%
Retail	98%

However, all the fraud prevention professionals we surveyed believe it's important[1] to consumers that the process of opening an account online is secure.

It's clear that fraud prevention professionals have a major task on their hands to develop robust identity verification solutions that are quick, easy and secure, all without adding friction that impacts the onboarding of good and great customers.

In fact, when asked what they consider to be the most important features and/or functionality of identity verification solutions, US fraud prevention professionals were most likely to say improving the customer experience (17%).

It's a tall order.

The question is, how can fraud, risk and compliance teams deliver security without hindering growth and transformation strategies?

Notes:

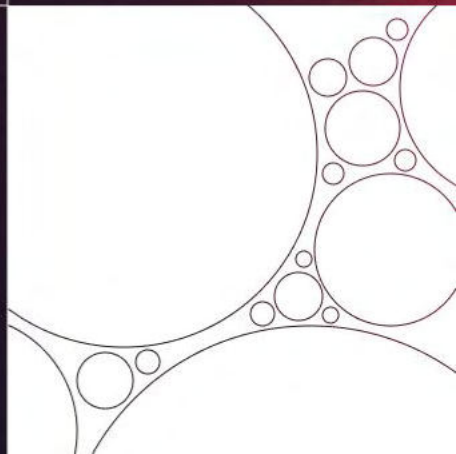
1. Reverse of 'At account opening – 1' (35%)
2. 'Extremely important', 'Very important', 'Moderately important' and 'Only slightly important' responses combined.
3. 'Extremely worried', 'Very worried' and 'Somewhat worried' responses combined.

CHAPTER 4

Joining forces to fight fraud

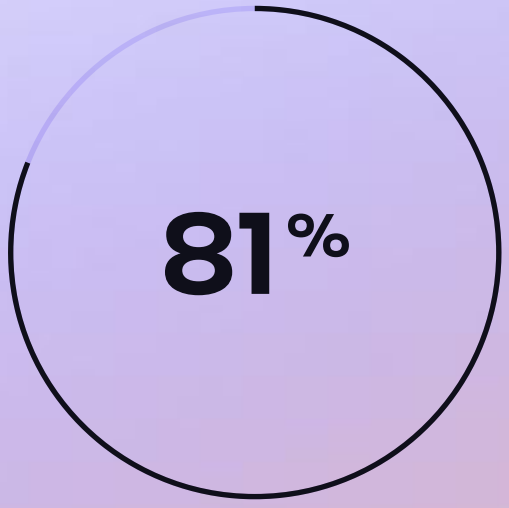
"Cross-sector data and intelligence sharing is essential. Only by breaking down these silos and working collaboratively across industries can we collectively protect individuals and businesses from the devastation of fraud."

Mike Haley
CEO, Cifas



If fraud is a global, cross-sector challenge, it follows that solutions should not be sought in isolation.

The clear majority of the fraud prevention professionals we surveyed agree. Eighty-one per cent believe that cross-sector identity intelligence sharing and collaboration can be a strategic differentiator in the fight against fraud across all industries.



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 (70%) are already part of an identity intelligence consortium/network that enables this collaboration, in practice their efforts are falling short.

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

UK	78%
France	90%
Germany	85%
Spain	86%

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

UK	64%
France	82%
Germany	85%
Spain	74%

78% agree[1] that organisations are letting down their customers by not prioritising cross-sector collaboration to combat fraud

76% agree[1] that organisations aren't doing enough to collaborate with other industries and organisations to help combat fraud

75% agree[1] that organisations are too worried about maintaining a competitive advantage to participate in cross-sector collaboration to combat fraud

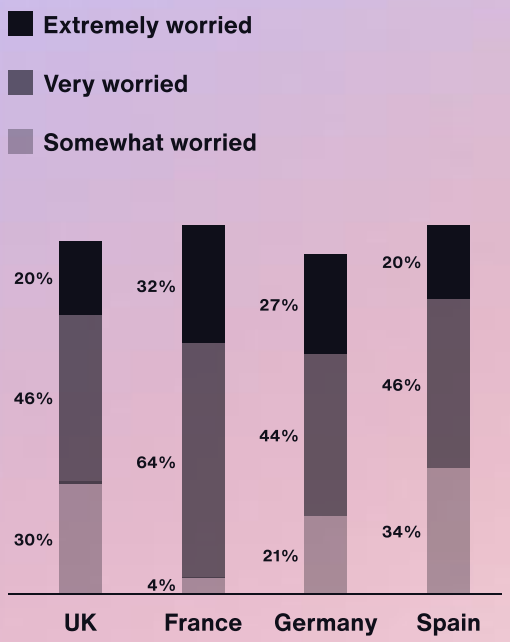
Many believe that regulators should be doing more with 4 in 5 (80%) agreeing[1] that governments around the world are not doing enough to support cross-sector collaboration to combat fraud.

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

	% of respondents[2]
Working better with organisations	51%
Enforcing regulation	49%
Setting clear standards on fraud prevention requirements	49%
Mandating cross-sector data and intelligence sharing	47%

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%).

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



Why wait for regulation to force your hand?

Notes:

1. 'Strongly agree' and 'Agree' responses combined.
2. Respondents who don't feel like the UK government is doing enough to help organisations fight fraud (19%).
3. 'Extremely worried', 'Very worried' and 'Somewhat worried' responses combined.

GBG TRUST

Building trust through onboarding intelligence

“With increasing public acceptance of advanced identity verification, building risk-based customer onboarding journeys that can flex to counter fraud signals will be the smart play in 2024.”

Gus Tomlinson
Chief Product Officer, GBG

Our research suggests that it's time for things to change.

Fraud, risk and compliance professionals 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 challenge is not confined to specific industries or regions but is common to all.

Increasing fraud is a global problem that requires a global solution. It's time for organisations in all industries across the world to set aside their misgivings on identity intelligence sharing and come together in a united defence against fraud.

While the concept of cross-sector identity intelligence sharing has arrived and many European businesses are already part of a network, now is the time for organisations to work more closely together to fully realise a common opportunity: to establish trust in digital identities at the point of onboarding, before fraud has a chance to negatively impact a business or brand.

Global challenges require a global solution. GBG Trust is a global identity network designed to combine the strength of what organisations know about their customers, delivering trust insights and fraud signals while ensuring complete data privacy and commercial security.

This unique data network combines over 100 million data attributes (and counting) contributed by a consortium of over 600 businesses covering 24 sectors in over 80 countries. It connects digital identity onboarding checks to a powerful network of shared identity intelligence, helping to recognise great, good and bad customers without delay at the point of onboarding.

With GBG Trust we provide businesses with onboarding intelligence to make the best decisions about the next generation of consumers. Our complete understanding of identity delivers unique and timely insights to confidently onboard good customers with limited data, reward great customers and reject fraudsters. To find out more about how GBG Trust can help you to detect and prevent fraud at the point of onboarding visit:
https://www.gbgplc.com/en/protect/trust/

Onboarding intelligence – is our collective term for a rich combination of identity data references, history and behavioural insights from multiple commercial and government sources. These insights help brands recognise good customer prospects and spot fraud signals from suspicious identities, blocking fraud *before* it's onboarded to their business.

"Through the level of fraud detected, GBG Trust paid for itself just 17 days post-implementation"

Leading UK Fintech

"GBG Trust reduced the wave of money mules being onboarded by over 70%"

Tier 1 Australian Bank

"GBG Trust revealed over 88% of identities with a low Trust Score were involved in bonus abuse fraud"

Leading iGaming firm

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