Smoothing the customer journey and preventing fraud

GBG

Key Findings

GBG and Censuswide surveyed 901 respondents from financial institutions (FIs) in five key European markets: the United Kingdom, Germany, France, Spain, and Italy to determine the common challenges FIs are facing in fraud prevention and detection in the customer journey.

This study analyses how FIs are structuring fraud processes and adopting evolving technology solutions, whilst balancing priorities of control and a strong focus on frictionless customer experiences.

1. Managing fraud losses in current businesses is of the highest priority for 93% of respondents.

2. FIs want to avoid on-boarding potential fraudulent customers during the application process but also want to limit the amount of friction in the customer experience.

3. Scams, data breaches, phishing, and third-party identity theft became top challenges in 2020, accounting for the highest fraud losses.

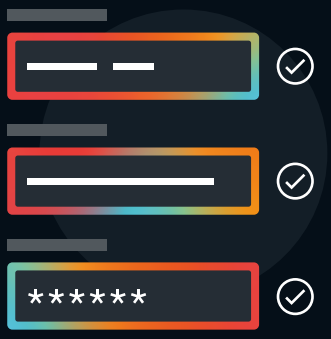
4. Investment has been budgeted for new technology by at least 96% of respondents, making technology a key priority in 2021.

5. AI and machine learning for detecting unknown fraud cases see greater demand and rollout by financial institutions who see them as fundamental for future-proofing fraud detection.

6. Italy, Germany, and Spain plan to invest more resources in 2021 in tackling endpoint threat detection, like digital fingerprinting, malware, and phishing.

7. Fraud and compliance operations are coming closer together; 28% of financial institutions admit full integration of processes at their organisation with a further 34% planning a full integration.

Customer onboarding processes to mitigate fraud and offer a smooth digital experience



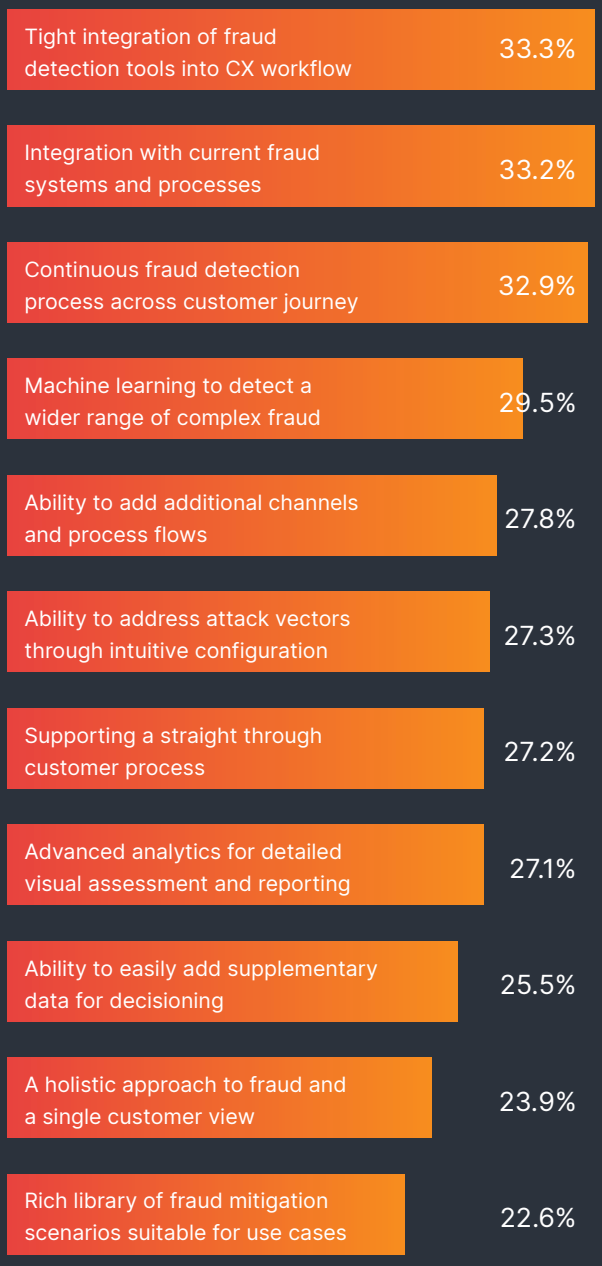
Essential features of ideal fraud technology

A significant majority (93%) of FIs agree that managing fraud losses is a key necessity and focus for business strategy. Successful fraud mitigation requires an intelligent way to smoothly onboard trustworthy customers whilst targeting threats that present clear risks. This frequently requires innovation in technology or processes with consideration for future-proofing also.

93% of FIs agree that managing fraud losses is a key focus for business strategy and guidance

Figure 1

Essential features of ideal fraud technology



Smoothing the digital journey

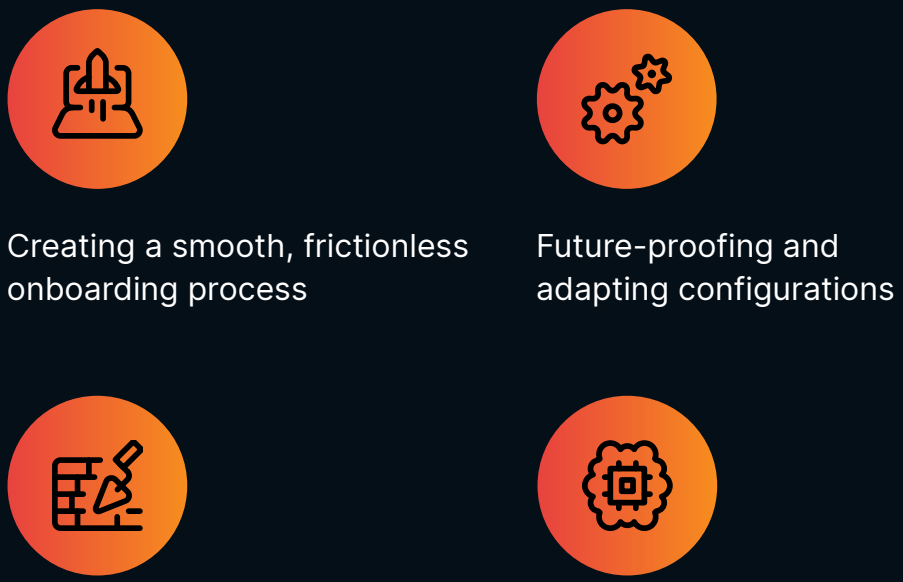
From the research, FIs are finding it more challenging to do fraud checks in the new customer application and digital onboarding processes than other parts of the customer journey. FIs want to smooth the onboarding process for customers but it can be difficult gathering information without creating customer friction. Accurate risk rating at the onboarding stage helps identify threat actors before the transaction stage.

33% of respondents want to use continuous fraud detection processes in the customer journey, tighten integration of fraud detection tools in the customer experience workflow, and integrate essential tools with current fraud systems and processes. FIs support a straight-through customer process, with the ability to introduce appropriate friction only when necessary by 27%. Respondents are considering new ways to improve fraud technology by considering machine learning and other advanced artificial intelligence techniques to detect a wider range of complex fraud behaviours and drive operational efficiencies (30%).

In Figure 2, FIs want to improve the customer journey in four ways: creating a smooth, frictionless onboarding process; future-proofing and adapting configurations; building both out-of-the-box and core features; and integrating AI and machine learning.

Figure 2

Improving the customer journey

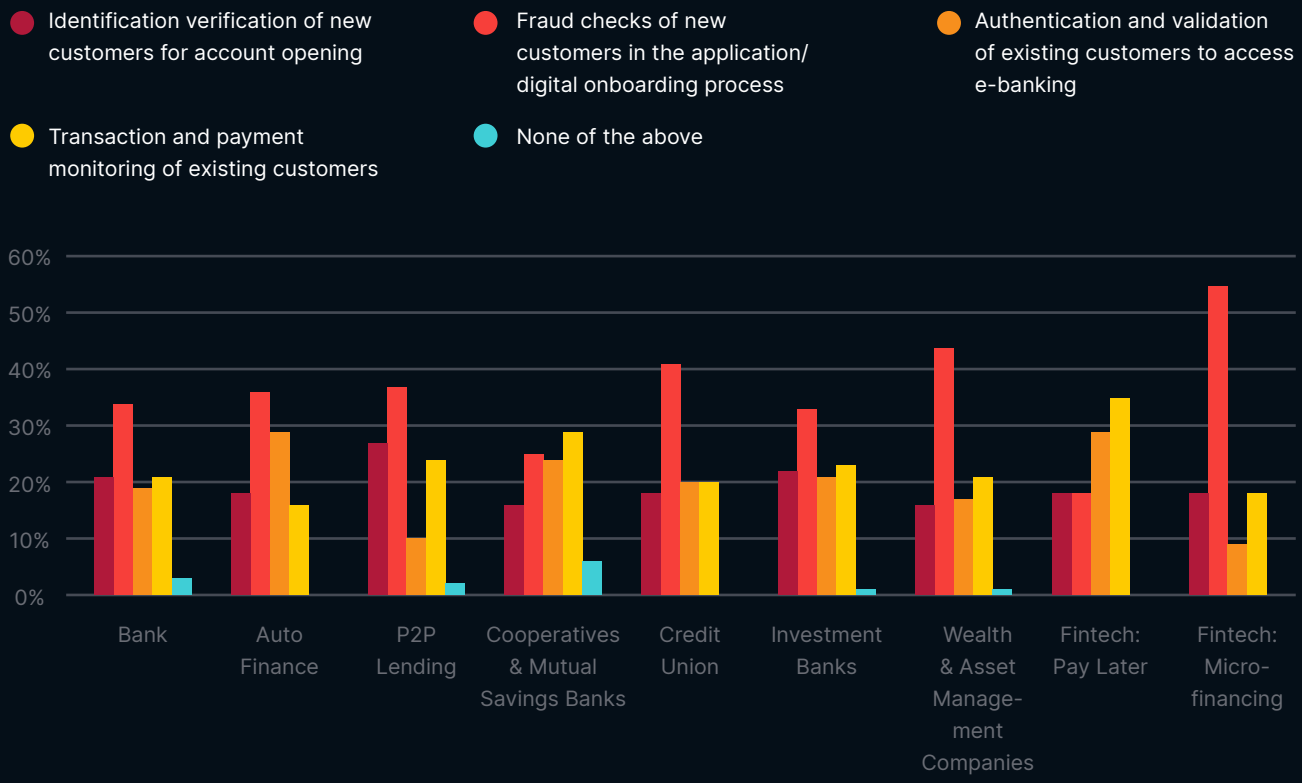


Ensuring a superior customer experience has always been an integral priority for FIs seeking to simplify the customer journey and looking to converge compliance and fraud with the ability to share information between units. More than 75% of respondents have either fully integrated fraud/compliance processes or are planning to integrate both in 2021.

Fully integrated fraud and/or compliance processes at only 28% of FIs, but 34% plan a full integration in 2021.

Figure 3

Customer journey challenges by industry



Across the fraud management customer journey, transaction and payment monitoring of existing customers is highlighted as a key challenge for the fintech sector (35%) and cooperatives and mutual savings banks (29%). Maximising efficiency in the end-to-end operation will be key for these two sectors for anti-fraud strategy.

Notable increases in fraud typologies for 2020

Variety and complexity of fraud increasing across board

Social engineering attacks are one of the most difficult types of crimes to detect, as they start with the manipulation of consumers to disclose their private data, and often involve the victims themselves in the act of committing the crime. Scams are an ongoing challenge with more than half of respondents observing an increase in frequency in 2020.

96% of respondents identified an increase in some type of fraud in 2020 whether that was scams or other types such as phishing or third-party identity theft. Traditional processes are no longer adequate—customers now require supplementary data to add important context to combat growing threats. With a multi-layered scoring approach, FIs can make better and more accurate decisions.

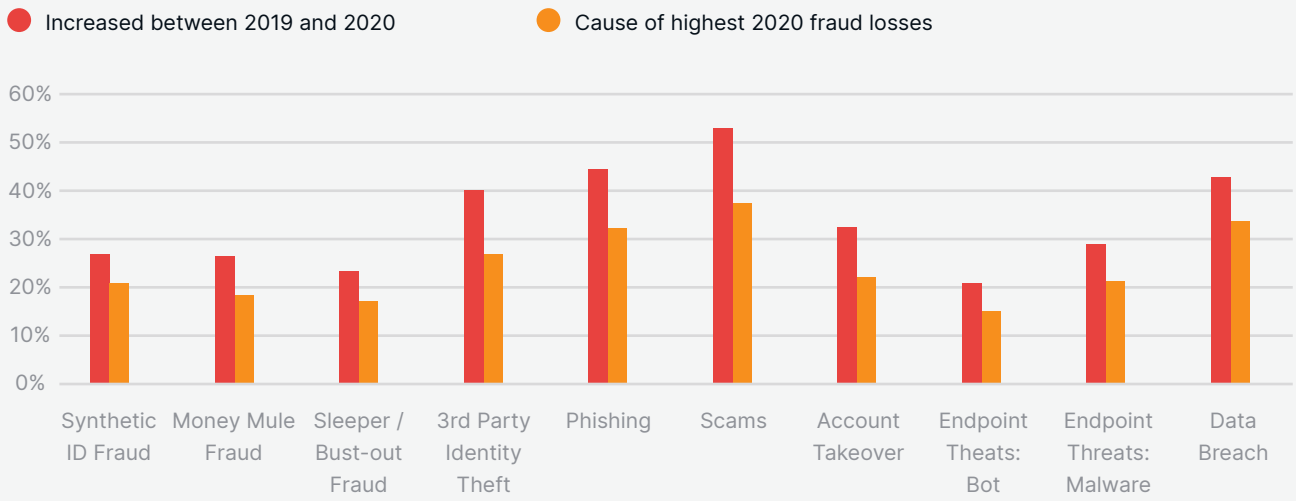
Each layer adds more context to a decision. Each layer adds further accuracy and power to detection. More layers, more value.

Cyber threats increase

Scams, phishing, account takeover, third-party identity theft, and other types of cyber schemes prey on the vulnerable and accounted for the highest fraud losses in 2020, according to respondents. Traditionally, the hardest fraud to detect is the one causing the biggest fraud losses. Using GBG's multi-layered approach to fraud detection—including data integration, risk-score assessments, machine learning, and alert generation—FIs can prevent cyber fraud sooner and reduce losses.

Figure 4

Increases in fraud types for 2020



The COVID-19 pandemic has also escalated the volume of cyber fraud attacks with increased online dependency. During the pandemic, cybercriminals have been seen advancing their capabilities, adapting quickly, and targeting relevant victim groups more effectively.[1] In an April 3 report, Europol suggests the COVID-19 outbreak has led to a significant upsurge in the total number of cyber attacks targeting public or private organisations and individuals. Europol has observed an intensification of ransomware attacks over the timespan of the pandemic outbreak and a spike in malicious domain name registration, whereas an escalation in Denial of Distributed Services (DDoS) attacks is expected in short or medium term.[2]

In Figure 4, respondents report that scams increased the most (53%) at their organisations in 2020. Scams also attributed to the highest fraud losses in 2020 by 37% of respondents. Though phishing is the second-highest fraud scheme increase reported (44%), data breaches accounted for the second-highest increase (34%) in fraud losses for 2020.

Scams: UK versus Italy

Scam cases increased 62% in the UK whilst respondents in Italy report a lower threat, with an increase of 36%. In the UK, 42% of respondents said that out of the fraud types, they attribute the highest percentage of their 2020 fraud losses to scams, whereas 20% of respondents in Italy said the same.

[1] Source: ENISA Threat Landscape 2020, Oct 2020

[2] Source: COVID-19: Amid a "Pandemic" of Cyber-Attacks, CyberTrust, April 2020

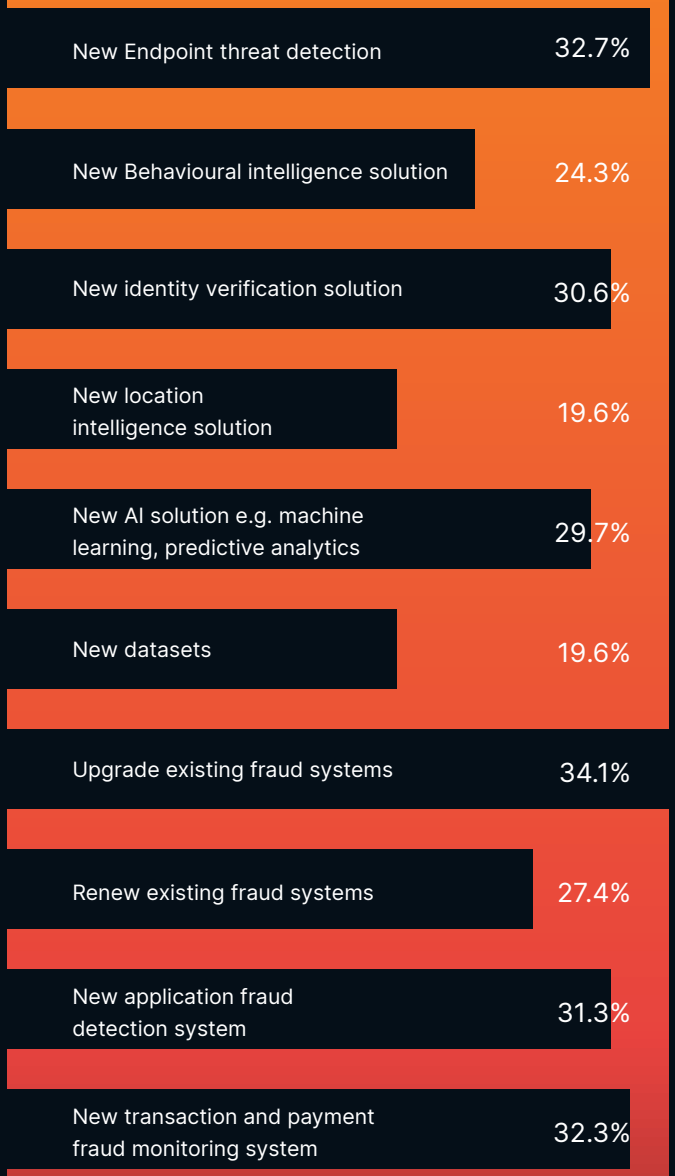
Fraud prevention and online fraud detection through new technology solutions

Investing in fraud management platforms

Having the right digital product mix and infrastructure to support the desired experience differentiate one financial service provider from another. Of the FIs surveyed, 96% plan on investing and prioritising new technologies and capabilities in 2021. The same percentage of respondents show a desire to tighten and improve fraud detection for their customers and see Machine Learning as a promising tool.

Figure 5

Planned investment in key technologies and capabilities



FIs are looking to invest heavily across multiple capabilities to help in the fight against financial crime. 33% want to invest in new endpoint threat detection, i.e. digital fingerprinting, malware, phishing, and more. FIs also plan to implement new transaction and payment fraud monitoring systems (32%), new application fraud detection systems (31%), new identity verification solutions, like eKYC and biometric systems, and new AI solutions, like machine learning and predictive analytics (30%).

AI and machine learning for detecting unknown fraud cases (52%) and future-proofing fraud detection (59%) see greater demand and rollout by financial institutions in the European region. Future-proofing fraud detection only works well with an adaptable configuration and models, which are core GBG offerings. Using GBG's multi-layered approach to fraud detection, FIs add accuracy and power to detection.

96% plan on investing in or prioritising new technologies and capabilities

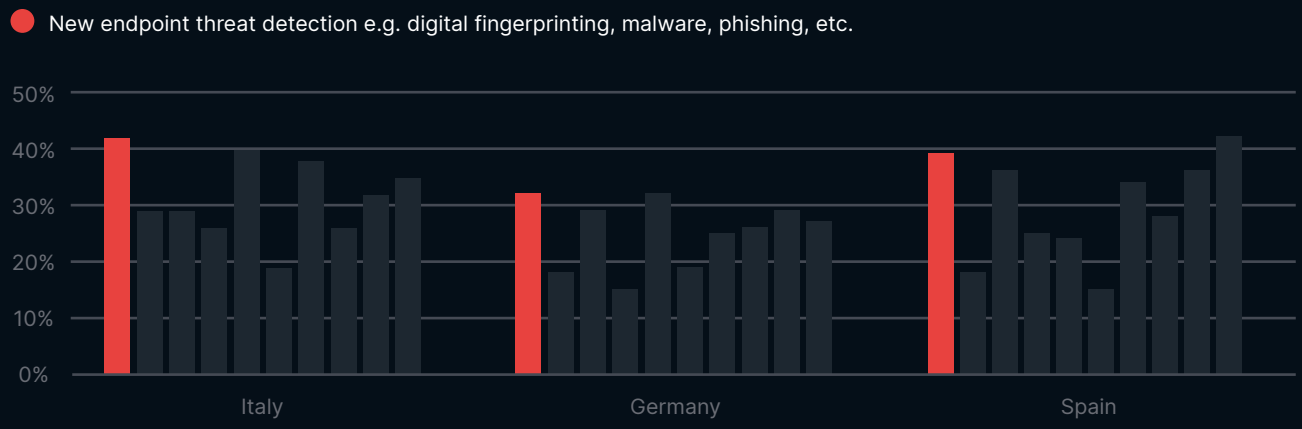
34% plan to upgrade existing fraud systems

24% plan to invest in new behavioural intelligence solutions

20% plan to invest in new location intelligence solutions

Figure 6

Countries looking to endpoint threat detection



In Figure 6, data shows that Italy, Germany, and Spain in 2021 plan to invest more resources to new endpoint threat detection, like digital fingerprinting, malware, and phishing. This data points to a different strategy for technology integration in these regions when compared to aggregate data as a whole.

Investment budget for technology implementation

On average, two of the European countries—Italy and Spain—are estimating a technology implementation budget between GBP2 million and GBP5 million. France and Germany are planning to spend more, on average, with an estimated technology implementation budget between GBP5 million and GBP20 million. The UK reported similarly high averages for both ranges, with plans to spend between GBP2 million and GBP20 million.

Figure 7

Estimated new fraud technology investment budget in 2020-2021

Breakdown across channels

FIs continue to maintain an omnichannel strategy to keep customers engaged whilst addressing pain points in a seamless and frictionless manner. On an aggregate across the European region, mobile banking and app banking are of equal importance to support retail-banking transactions.

Having the right digital product mix and infrastructure to support the desired experience differentiate one financial service provider from another. Shoring up existing fraud systems and investing in new technology ensure seamless end-to-end fraud and compliance risk management in the digital product preference.

Figure 8

Channel preference in the European region

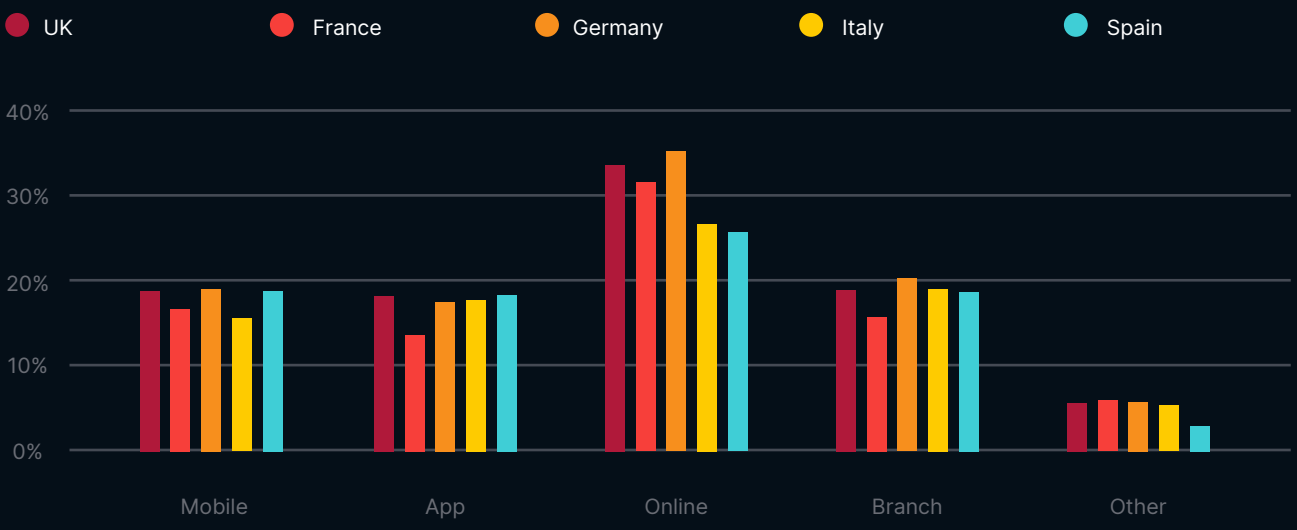
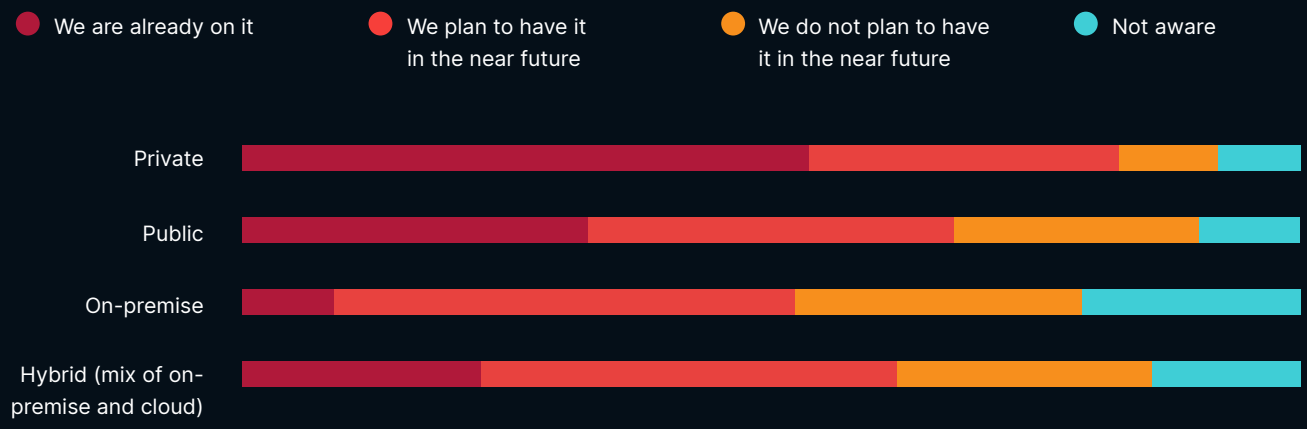


Figure 9

Cloud-hosted fraud detection solution



Cloud-hosted solutions

There is an apparent inclination towards using cloud-hosted fraud detection solutions. Private cloud is the preferred option by more than half of organisations, with more private cloud fraud detection application planned for by 29% of respondents. FIs (44%) are weighing the possibility of opting for an on-premise only cloud architecture system.

A hybrid cloud solution looks to overtake the preference for a public-cloud solution, with 23% of respondents already on it and 39% planning for it in the near future.

Private cloud deployment is the preferred cloud architecture system by 83%

Conclusion and recommendations

FIs in the European region want to grow whilst ensuring they are protecting their business and their customers. Offering a smooth digital journey is of the utmost importance on this track, but it's a balancing act—successful fraud mitigation requires an intelligent way to both onboard the vast majority of quality customers whilst introducing appropriate safeguards to ward off threat actors that present clear risks.

As fraudsters move to social engineering to digitally achieve their criminal means, and as the variety and complexity of fraud increases across the board, FIs are embracing new technologies to future-proof their fraud detection and reduce losses. Further compounding the situation, the global outbreak of the novel coronavirus has forced FIs in the European region to ramp up and embrace a fuller spectrum of digitalisation in a short time.

New-Gen sustainability

Financial crimes typologies require a new generation of fraud management technology. FIs are no longer looking just for simple technology solutions—institutions want modular technology with advanced data analytics and intelligence solutions.

Multi-layered scoring

Traditional processes are no longer fit for purpose. The GBG multi-layered scoring approach uses a multitude of "layers"—data integration, risk-score assessments, machine learning, alert generation—combined to generate an overall risk score, helping FIs make better and more accurate decisions.

Data intelligence

GBG's extensive data and intelligence sources add another layer to the fraud risk assessment scoring process. There is strength in data and derived intelligence from data. Derived data adds intelligence into scoring to more accurately drive decisions and processes, and make alerts more reliable.

About GBG

GBG (AIM: GBG) is a global technology specialist in fraud, location and identity data intelligence with offices in 18 locations worldwide. For over 30 years, GBG has been accessing and verifying identities, to the standards set by financial regulators, of more than 4.4 billion people worldwide or 57% of the world's population. GBG has a network of over 270+ global partnerships and access to 510+ datasets to provide data with accuracy and integrity.

In the fraud category, GBG manages end-to-end fraud and compliance needs across a range of industries including financial services (international, regional and local banks, auto finance, P2P lending, mutual companies, and credit unions), insurance, government services, retail, betting and wagering.

For more information

gbgplc.com/global

contact@gbgplc.com

GBG locations

APAC

Beijing, Canberra, Jakarta, Kuala Lumpur, Melbourne, Shanghai, Shenzhen, Singapore, Sydney

EMEA

Barcelona, Chester, Dubai, Edinburgh, Germany, Liverpool, London, Nottingham, Turkey, Worcester

USA

Atlanta, New York, San Francisco

GBG