UK banking fraud sentiment index

2023

pwc

In collaboration with DataEQ

DataEQ

Contents

Foreword 3

Introduction 4

Key themes and findings 5

Industry overview 6

Risk factors 11

Fraud reports 17

Servicing fraud reports on social media 28

Conclusion 32

The way forward 34

Methodology 35

Foreword

We are delighted to present the results of our UK Banking and Fraud Sentiment index, developed in collaboration with DataEQ. This innovative analysis brings new insight into consumer experiences of fraud and how banks, building societies and payment service providers (PSPs) are supporting customers. We've analysed social media interactions between consumers and 18 UK banks, building societies and PSPs over a three-year period, bringing a fresh perspective on the constantly evolving world of fraud risk management and the impact counter-fraud controls can have on customer experience. In doing so, we highlight some of the practical steps that can be taken to improve customer experience and how social media data can be used to provide real time insight into fraud trends and the impact of counter-fraud controls.

This report comes at a time of increasing government, regulatory and public attention on fraud. The role that banks, building societies and PSPs play in protecting consumers from fraud threats is getting more focus than ever. Rising rates of reported fraud and the explosion of scams are driving the introduction of new legal and regulatory obligations and new investment in counter-fraud measures across the industry. While headline rates of fraud remain high and there is clearly a need for further action, the level of engagement and investment in counter-fraud activity is encouraging.

Banks, building societies and PSPs play a crucial role in tackling fraud. Across the industry there is continual investment to improve counter-fraud measures, and the adoption of new technologies and safeguards to maintain levels of defence is a constant arms-race against the fraudsters. New regulatory obligations like the UK Payment Systems Regulator's mandatory reimbursement regime for scam victims will further strengthen consumer protection provided by the banking and payments industries.

Yet, as the analysis in this report shows, consumer perception towards banking service providers' role in protecting them from fraud is often negative. Effective fraud countermeasures are a baseline customer expectation and the benefits of the protections that banks provide to their customers can be lost in the noise. Social media should not be the only source to evaluate customer perceptions, but it does provide a different and underutilised perspective on an important and growing customer segment. While we might expect social media to more often be a platform for complaint, some banks have managed to drive positive sentiment through proactive engagement with the channel.

Most fundamentally, as a society, we would all benefit from a shift towards ever closer collaboration between banking service providers and customers to defeat the common adversary: the fraudsters. Banks and payment firms will increasingly need to engage actively with their customers on fraud threats; to work more closely together to capture and share intelligence when fraud cases are identified to provide real-time intelligence in counter-fraud processes; and to engage with law enforcement to support the disruption, pursuit and prosecution of criminal gangs engaged in fraud.

For this shift to take place, firms will need the trust of their customers. This analysis shows that there is real room for improvement when it comes to firms providing a positive experience for customers who have been the victim of fraud, and by making such an improvement, further gains in the fight against fraud should then come within reach.

Introduction

Fraud has emerged as a rising concern for UK consumers, with 3.5 million fraud offences reported in the year ending March 2023[1] and UK payment firms reporting that fraudsters stole more than £1.2bn in 2022[2].

Banks, building societies and PSPs have channelled significant investments into their ongoing battle against fraud in an ever-evolving world of digital banking. While headline rates remain high as fraudsters adopt new technologies and techniques to exploit changing vulnerabilities, investments in counter-fraud measures have delivered results with sustained reductions in certain types of fraud evident in the statistics. Despite these substantial investments and examples of success, consumer sentiment towards the handling of fraud by banks and PSPs remains largely negative.

A multifaceted threat, fraud is shaped by shifting consumer behaviours, emerging business procedures, developing technology and mutating fraud tactics. Addressing the proliferation of fraud demands a multifaceted response that fully encapsulates the intricate nature of the issue. Maintaining effective counter-fraud measures in this context while also providing a good customer experience is a delicate balance.

Rising fraud rates have driven greater political, regulatory and consumer pressure on banks and PSPs to enhance fraud countermeasures and their focus on protecting consumers, especially when handling fraud. Drives to strengthen fraud prevention can lead to unintended consequences for the customer: Most notably, higher friction in payment journeys and the risk of restricted access to banking products or services.

Social media platforms are becoming the stage for more and more consumers to broadcast their experiences, most often perceived negative or unfair experiences, and in doing so, making these visible to the wider online community. Social media data represents an expansive and underutilised source that can be analysed in real-time to provide feedback on crucial themes related to fraud conversations, providing insight into the equilibrium of fraud control and customer experience.

The UK Banking Sentiment and Fraud Index, a collaboration between PwC and DataEQ, analyses consumer sentiment towards 18 of the country's banks, building societies and payment firms (which we will collectively refer to as "banks" throughout the rest of this report) through the lens of consumers and their social media posts. The analysis is based on 1.5 million social media mentions about these firms between May 2022 and April 2023, focusing on the conversations within that population relating to fraud.

This index delivers findings that enable firms to pinpoint the root causes of their negative sentiment. Data-driven insights provide a clearer understanding of customers' process and communication pain points, identifying areas where they feel banking service providers could perform better.

[1] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2023

[2] https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2023

Key themes and findings

Along with general banking volume, fraud conversations have shown a YoY increase

Fraud conversation within UK banks' social media has grown YoY

General banking conversation has also seen a steep rise year-on-year, indicating social media is a key area for banks' monitoring and response.

Consumers hold banks accountable for fraud

Consumers hold banks accountable for fraud

Outrage targeted at banks on social media shows that customers do not see banks as passive third-party service providers when fraud issues arise. Banks can redefine the narrative to one of partnership against fraudsters.

Banks need to offer a range of channel options for reporting fraud

Call centres face challenges in effectively managing fraud reporting

A variety of digital channels is needed to provide the right support to diverse victims.

Failing to respond to customers on social media puts them at risk of being targeted by fraudsters again

There is a risk that fraudsters may take advantage of banks' silence on social media

Timely responses are crucial to prevent potential fraudsters hijacking conversations at a time when customers may be more vulnerable to scams.

Fraud experiences shared on social media undermine banks' reputations

Fraud experiences shared on social media undermine bank's reputations

Customers will use social media, irrespective of bank's preferred channels. Bank's must engage where their customers are to protect their reputation.

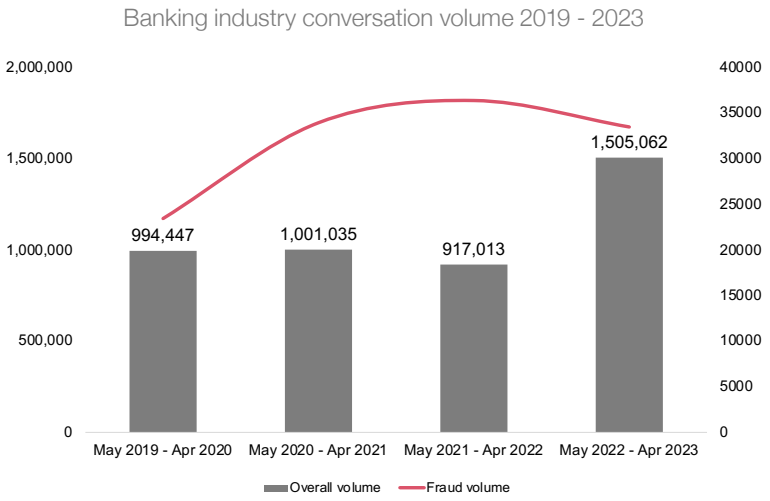
Strategies to mitigate and efficiently handle fraud can drive positive sentiment

Strategies to mitigate and efficiently handle fraud can drive positive sentiment

Customers value visible actions like strengthened security protocols and public education strategies, as well as consistent feedback to their posts.

1 Industry overview

Since 2019, chatter on X (formerly known as Twitter) about UK banks has increased by over 50%. This surge in social media activity has correspondingly led to a rise in fraud-related discussions, which have grown by 35%. From May 2022 to April 2023, there was a significant upswing in social media conversation related to the UK banking industry.



50%

Twitter conversation about banks has increased by over 50% since 2019, with fraud conversation growing by 35%.

While the increase in conversation will be driven by several factors there are four macro trends that are likely to be contributing:

Changing customer attitudes

While social media users were once focused within younger age-groups, over time adoption has spread through a wider demographic with these platforms becoming more established and accepted channels for business engagement. This has driven a general increase in the use of social media platforms, in turn leading to more conversations about banks and fraud.

A shift in banking

More and more banks are moving their operations online. This pushes customers towards social media, turning it into a key communication hub.

The cost factor

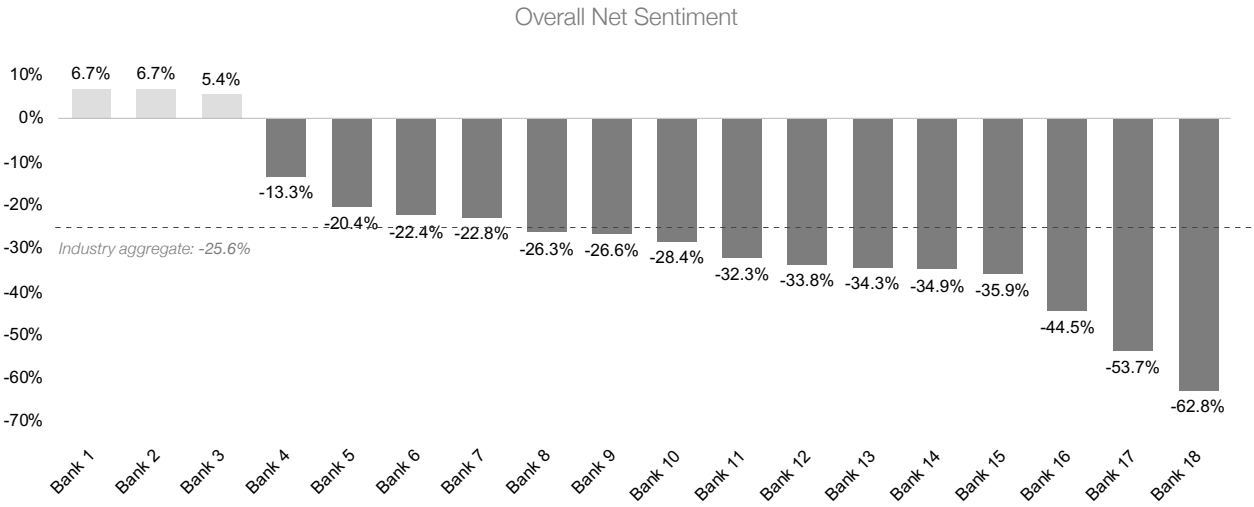
As some banks reduce or eliminate the provision of phone support, customers are turning to alternative channels to quickly contact their banks, using the visibility that social media provides to provoke a faster response.

Searching for human help

When faced with automated responses at call centres, customers can feel overlooked. So, they are taking their conversation online, where they feel there's a better chance of connecting with real people.

Digital challenger banks claimed the top 3 positions with an overall positive Net Sentiment score

Net Sentiment, an aggregated customer satisfaction metric calculated by deducting negative sentiment from positive sentiment, highlighted challenges faced by the UK banking industry. Of the 18 banks in the Index, 11 recorded Net Sentiment scores beneath the industry aggregate of -25.6%, with the lowest scoring bank registering -62.8%.



Excludes enterprise mentions

Leading causes of this negative Net Sentiment came from customers expressing dissatisfaction with online and digital reporting channels, poor customer service, as well as payment and servicing issues.

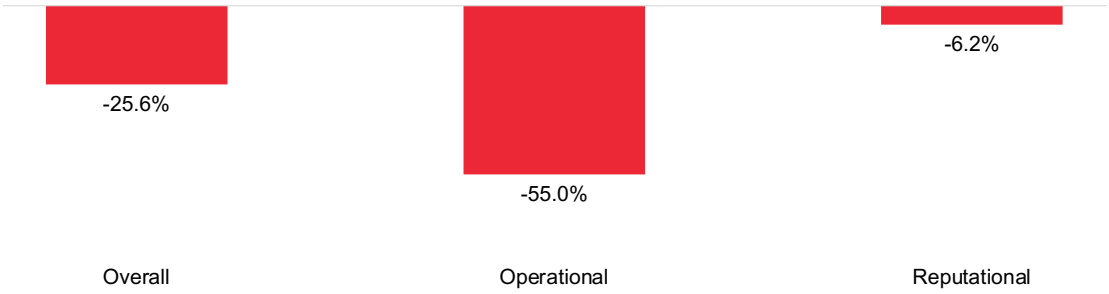
Three of the banks did however manage to achieve a positive score – highlighting that while social media is more often a platform of complaint, positive brand perceptions can be achieved. Two banks tied for first at 6.7%, placing them 32.3 percentage points above the industry aggregate. These banks enjoyed a considerable share of positive feedback from customers applauding features within their banking apps, sharing their positive personal experiences, and recommending the brand to others.

Operational complaints diminished overall Net Sentiment

The overall Net Sentiment score comprises two categories of conversation, operational and reputational. Operational conversation includes mentions where the author can be identified as being on the customer experience journey, anywhere in the process from pre-customer to post-customer, while reputational conversation includes mentions about brand-driven content, promoted services, and associated corporate social responsibility (CSR) activities.

Operational Net Sentiment for the UK Banking industry came in at -55%. The negativity in this category overshadowed the -6.2% sentiment score attributed to reputational aspects such as marketing campaigns or other reputation-related events.

Banking industry Net Sentiment breakdown



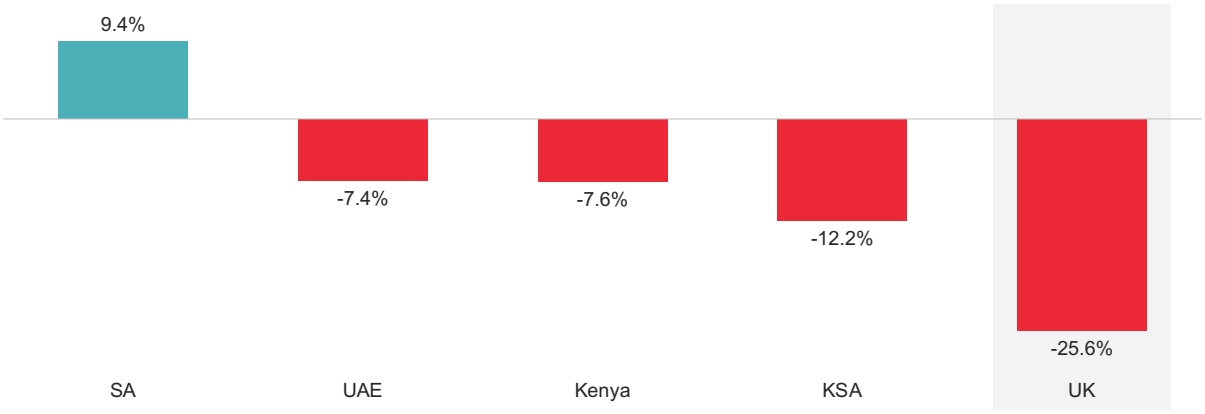
Despite the potential for reputational sentiment to offset negativity in overall Net Sentiment, this was not the case for the UK. This presents an opportunity for UK banks to leverage social media to positively influence consumer perceptions of their service and reputation.

DataEQ analyses social media conversation in various other banking industries and has conducted similar studies in South Africa, Kenya, the United Arab Emirates and the Kingdom of Saudi Arabia. The results in these countries showed how these banks have used focused marketing campaigns to incentivise the sharing of positive customer experiences via social media, resulting in more positive operational conversation.

UK banking's overall Net Sentiment trails behind other banking markets measured by DataEQ

The UK banking industry is seeing a lot of change and falling under constant scrutiny - including on social media. While it's not uncommon for banks to score negatively in Net Sentiment on social media, the UK industry's sentiment is considerably behind those within other countries analysed by DataEQ.

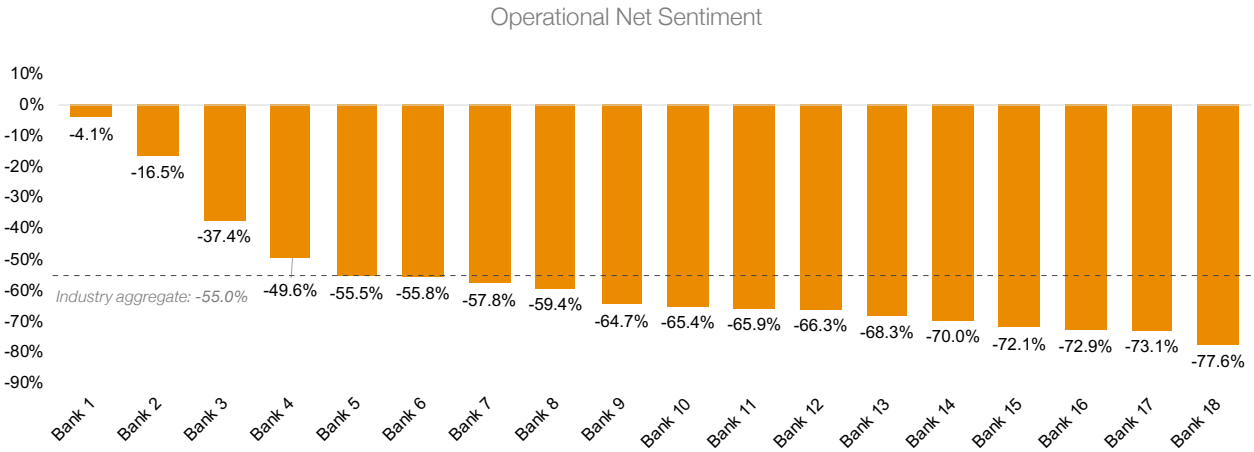
Regional view: Overall Net Sentiment



It's also worth considering the perceived general distrust in institutions. The banking industry, inherently tied to people's lives and livelihoods, is not immune to this sentiment. This could indicate lingering trust issues, possibly a hangover from past financial crises. On top of that, perceived mismatches between higher mortgage rates versus lower savings rates are driving discontent. This scepticism and dissatisfaction could be manifesting in the ongoing conversations around the industry.

The fraud experience impacts the sentiment towards the broader customer experience

When looking at operational Net Sentiment, all 18 banks scored negatively. This is unsurprising, as people predominantly use social media as a place to raise complaints when things go wrong during the customer journey. Being a victim of fraud is understandably a significant low point in any customer's experience. As such, the way banks respond to consumers' reports of fraud can have a long-lasting effect on the broader customer experience.



Excludes enterprise mentions. Operational conversation considers individual mentions from those in the customer journey

The leading bank for this metric recorded an operational Net Sentiment rating of -4.1%. Despite this being a negative score, it was markedly less negative than the industry aggregate of -55%.

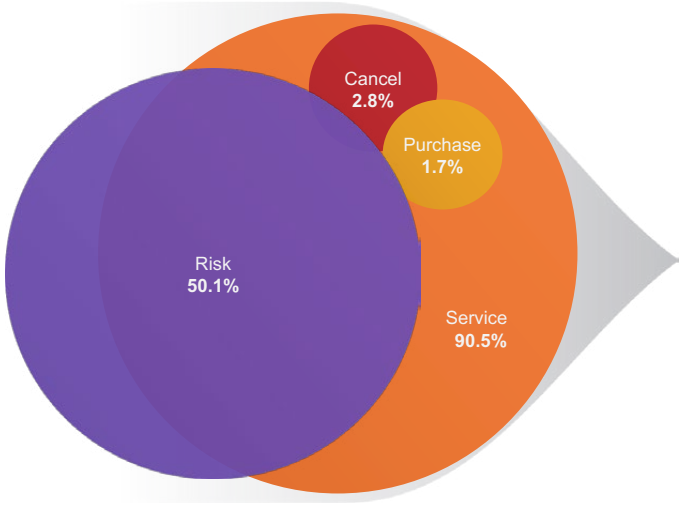
Established banks must not overlook their challenges in operational engagement. The ever-increasing reliance on social media and the influx of younger, tech-savvy customers necessitates a proactive approach to managing the bank's public image.

Negative sentiment, if allowed to fester, can become entrenched in consumers' perception, potentially inflicting severe damage to the institution's reputation. It's crucial for banks to foster a more positive sentiment before reaching a critical tipping point in the cultural zeitgeist, where they risk becoming a meme associated with poor service.

2 Risk factors

Mentions that pose a potential brand risk are identified by DataEQ among other high-priority conversations, referred to as “RPCS conversations”. These are the mentions that matter, and the ones that banks should pay most attention to.

RPCS conversations should be considered by banks for priority response



Risk factors:

- Discrimination
- Downtime
- Protests or boycotts
- Health, safety or security
- Accusations of unethical behaviour
- Threatening regulatory or legal action
- Claims
- Fraud reports
- Anti-competitive behaviour
- Escalation

DataEQ defines RPCS (Risk, Purchase, Cancel, Service) conversations as:

Risk
Mentions that pose an operational or reputational risk for the brand.

Purchase
Mentions from prospective customers who want to purchase products or services.

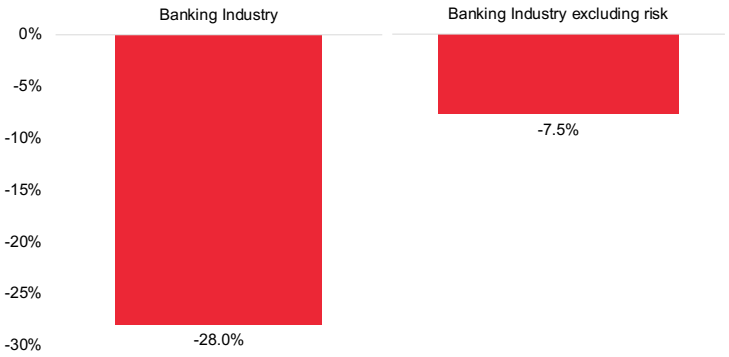
Cancel
Mentions from customers looking to cancel their service or not purchase from the brand again.

Service
Mentions from customers who require assistance or describe an experience with the brand.

Both operational and reputational risk conversations made significant contributions to industry perceptions.

Risk conversations negatively impacted the banking industry's sentiment by more than 20 percentage points. The majority of risk discussions being operational in nature presents an opportunity for banks to intervene shortly after the problem is reported. This shows the importance of monitoring social media in order to be aware of issues and minimise their negative impact.

The impact of risk on Net Sentiment for the banking industry



Verified non-enterprise mentions, excluding reshares

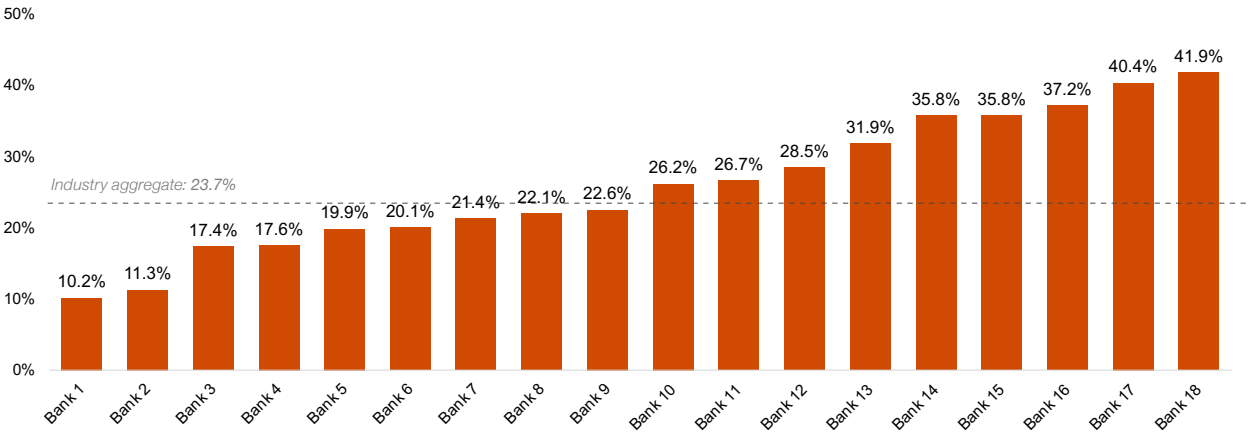
20 pp

Risk conversation dented the banking industry's sentiment performance by more than 20 pp.

Just under a quarter of all consumer conversations contained a risk theme

When looking at the proportion of risk volume for each bank in relation to their overall conversation volume, the two leading banks for this metric stood out with only 10.2%, and 11.3% respectively - well below the industry aggregate of 23.7%.

Risk conversation as a proportion of overall volume per bank



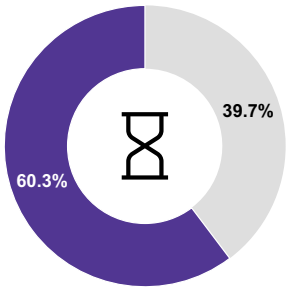
Verified non-enterprise mentions, excluding reshares

When looking at the proportion of risk volume for each bank in relation to their overall conversation volume, the two leading banks for this metric stood out with only 10.2%, and 11.3% respectively - well below the industry aggregate of 23.7%.

Common themes in risk conversation across all banks included poor communication and customer service. Consumers were concerned when their banks did not provide public updates regarding widespread downtime issues, resulting in fear for the safety of their finances. Allegedly impolite, unhelpful, or unresponsive customer service agents saw consumers posting their complaints on public platforms which could turn potential customers away.

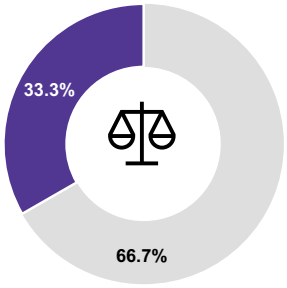
Top three drivers of risk conversation:

Fraud had the lowest proportion of conversation but posed the most significant reputational risk



Downtime

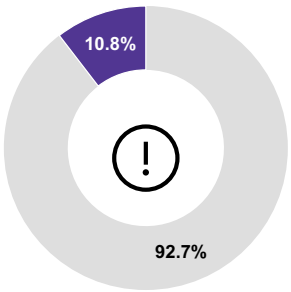
Making up 60.3% of risk volume, downtime complaints were focused on prolonged periods of unavailability to banks' web or app services. Banks' silence on downtime causes and resolutions elevated customer frustration. Furthermore, complaints about discourteous or unresponsive agents led customers to vent on public platforms, potentially deterring prospective customers.



Perceived unfair treatment

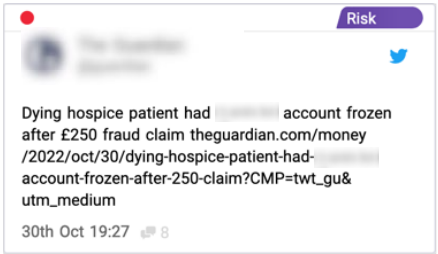
Reports of unfair treatment made up 33.3% of risk volume. Customers aired grievances about unexplained account blocking, inaccessible services, miscommunication, and incorrect refunds.

The absence of public updates during downtime sparked fears about financial security, with customers expressing concerns about being able to pay their bills on time. Some customers levelled accusations of theft at bank agents, while others threatened to move their accounts to other banks.



Fraud reports

Fraud reports constituted 10.8% of risk conversation volume. Fraud, as a risk factor, carries substantial weight on a brand's reputation. Fraud reports were not confined to limited social media mentions, but also found their way into higher visibility press reports.



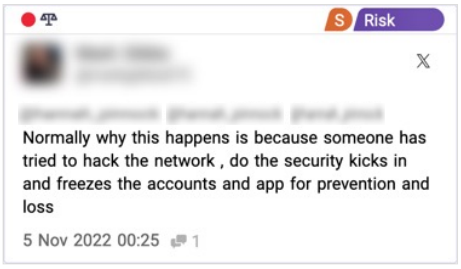
Correlation seen between downtime and security or fraud concerns

Customers unable to access their accounts most often attributed this to downtime rather than suspected fraud-induced account freezes. Consumers reported being unable to log in to their banking apps or online profiles for several days. Many wanted to know if they would be compensated for any costs they incurred during the period.

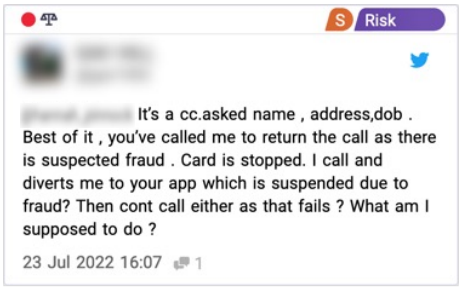
> Most banks saw complaints about blocked or frozen accounts.

A lack of communication exacerbated concerns about staff conduct and competency, as well as fears about financial safety.

Concerns about security surrounding downtime

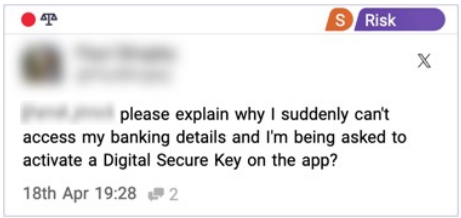


Downtime preventing fraud reporting



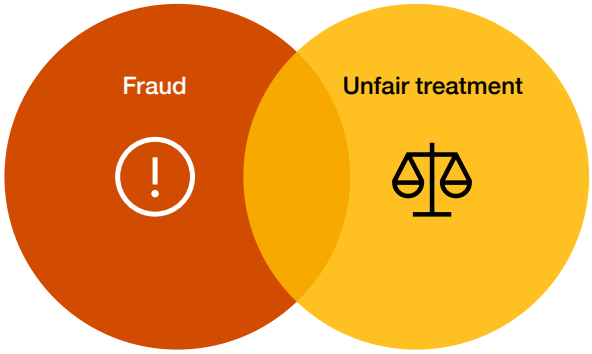
Downtime associated with security issues

Frozen accounts/fraud mistaken for downtime



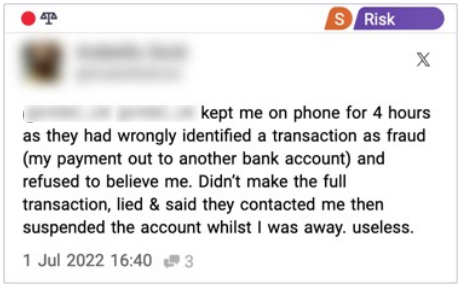
Failures in expectation management and fraud support processes left customers feeling unfairly treated

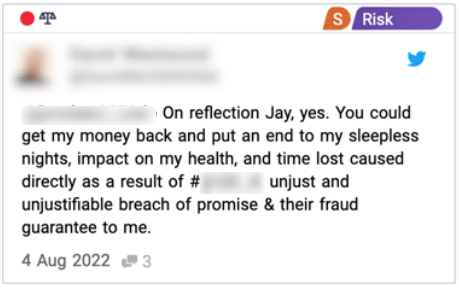
Banks were accused of closing or freezing accounts for unwarranted reasons and unfairly preventing customers from accessing their funds. Attempts to reopen or unfreeze accounts were allegedly met with poor responses.

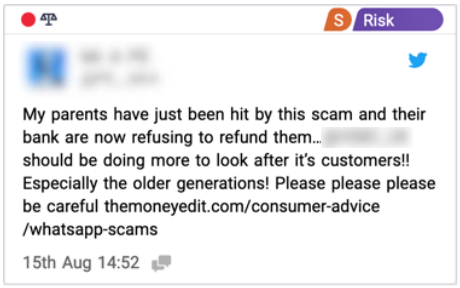


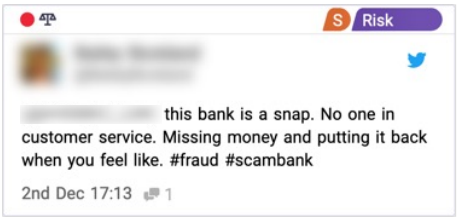
The issue of frozen or blocked accounts remained prominent in risk conversation across multiple topics.

A lack of public acknowledgment or satisfactory responses led to heightened accusations of theft, fraud, and money laundering, resulting in calls for boycotts and threats of legal action.





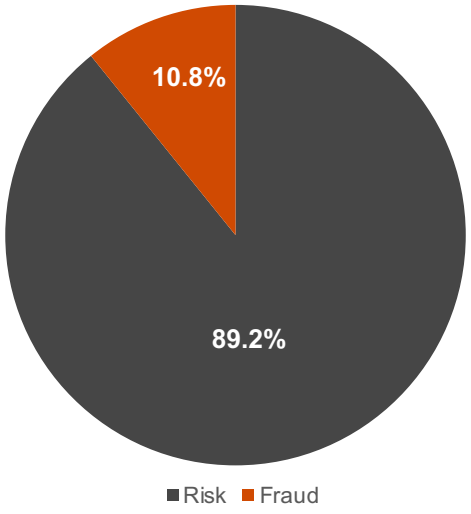




3 Fraud reports

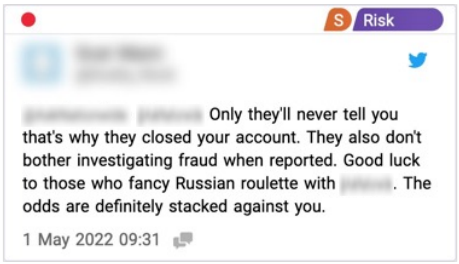
Risk conversation is further separated by the DataEQ Crowd, into risk-related topics, allowing a more granular view of the data. This section will take a deeper-dive into the fraud conversations to explore the nuances of this complex topic.

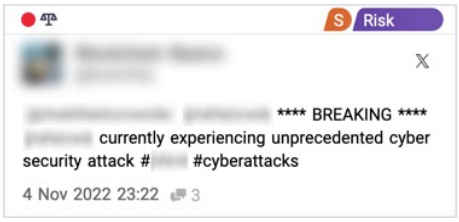
Percentage of fraud mentions in risk conversation



Verified non-enterprise mentions, excluding reshares

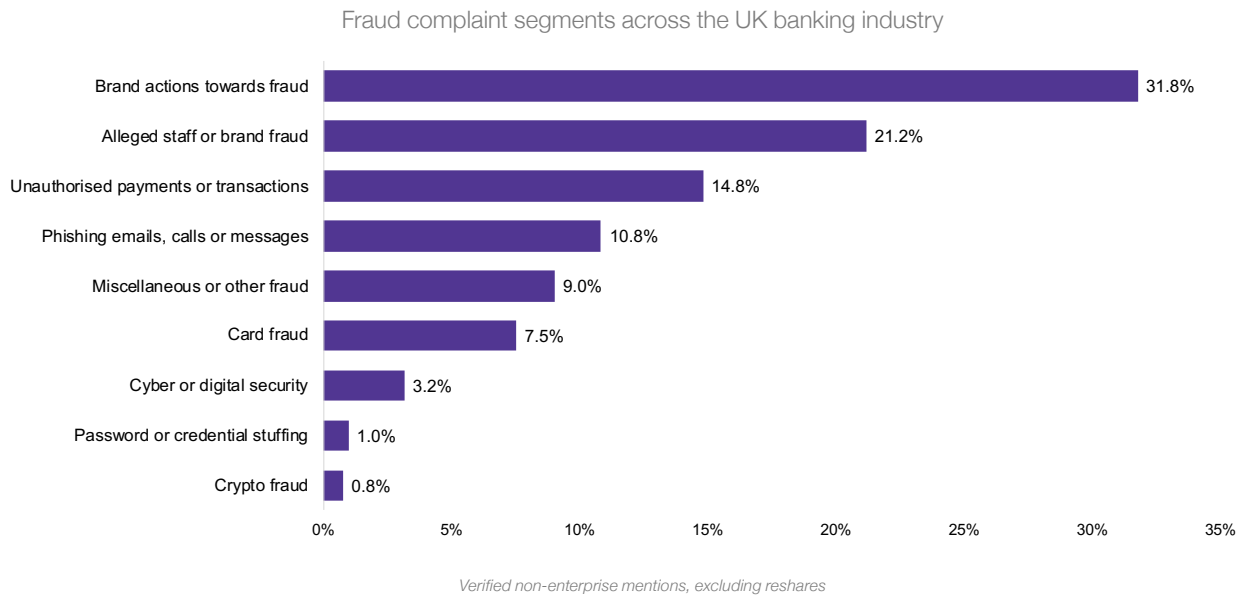
Despite only accounting for 10.8% of overall risk volume, fraud conversation can have a significant reputational impact on banks due to the sensitivity that typically surrounds the topic.





Consumers alleged that brands were not doing enough to counter fraud

This graph displays the distribution of fraud conversation across the nine identified types of fraud. The main grievance centres on responses to fraud. These conversations show how consumers scrutinised banks' actions, or perceived lack thereof, in mitigating fraud or managing fraud-related complaints.



The second-most reported type of fraud was alleged brand or staff fraud, which included client theft incidents.

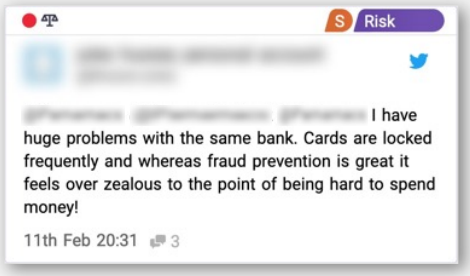
Unauthorised payments or transactions were the third most prevalent topic of fraud conversation. This included instances where consumers reported unrecognised transactions or disappearing funds from their accounts.

31.8% The most prominently complained about topic was that of brand actions towards fraud.

Exploring the criticism of brands' action towards fraud

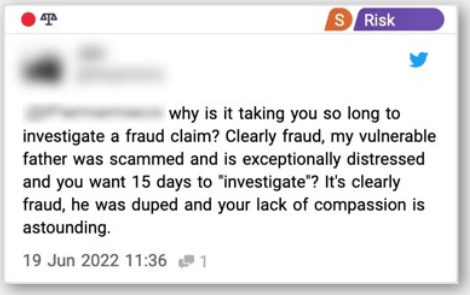
This section delves into the common grievances expressed by customers across multiple banks in the UK banking industry. These mentions offer vital insights into the consumer sentiment surrounding the sector and how banks can improve their response to fraud or suspected fraudulent activities.

Banks were too quick to block accounts due to suspected fraud



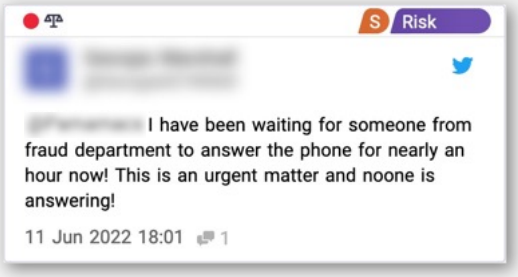
Many customers expressed discontent over hasty blocking or freezing of accounts due to potential fraud, often disrupting genuine transactions and leading to stressful unblocking procedures. This illustrates the delicate balance between the robustness of controls and customer experience and is an example of a situation where banks can emphasise that actions are driven by a desire to protect their customers.

Perceived impolite and unhelpful staff compounded the anxiety of fraud victims



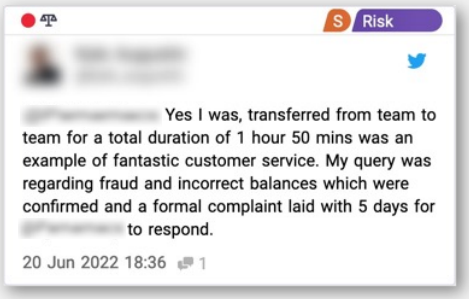
Staff handling customer fraud reports were often perceived as impolite and unhelpful. This heightened victims' already high-stress levels. In the worst-case scenario, customers felt that they were being treated with suspicion when they were reporting being a victim of fraud. Enhanced employee empathy training could help alleviate this issue by allowing consumers to feel more secure when reporting possible fraud. More broadly, developing procedures that reinforce the importance of the bank and the customer working together to prevent fraud is key.

Slow turnaround times increased unease over financial impact of fraud



Extended hold times, delayed investigations, and infrequent updates further increased customers' anxiety about their financial stability. Mechanisms to provide feedback and engage with customers on the status of fraud cases could reduce these concerns, and strengthen the sense of collaboration.

Multiple transfers between departments highlight bottlenecks in interdepartmental communication



Customers reported being repeatedly transferred between departments when dealing with fraud cases. Some customers said they had flagged suspicious transactions but that nothing was done to stop them, and that they had to provide the same documentation several times. This indicates communication and procedural inefficiencies across organisations. Optimising processes to minimise handoffs between teams and creating capabilities to handle customers' concerns at the first point of contact where possible are key.

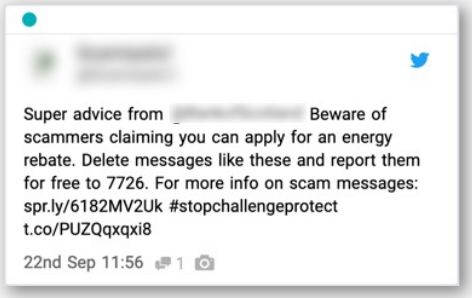
Some bank responses to fraud were appreciated by the public

Despite the general negativity surrounding fraud discussions, some actions by banks were favourably received. Positive conversation relating to fraud was identified by DataEQ using key phrase matching, including retweets and reshares, represented by four categories.

These four categories of conversation indicate that consumers are seeking reassurance from their banks, and are aware of the significant role that banks play in mitigating fraud.

Public education

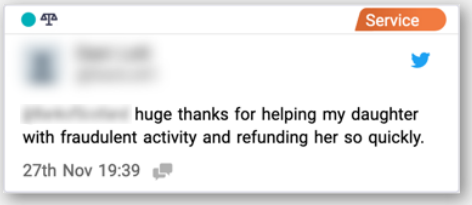
Consumers responded positively to any attempts to inform the public about scams, security measures etc.



Banks received positive feedback for initiatives aimed at educating the public about digital security, common scams like romance-fraud, and other anti-fraud measures. This includes promotion of initiatives like the #StopChallengeProtect campaign.

Quick responses

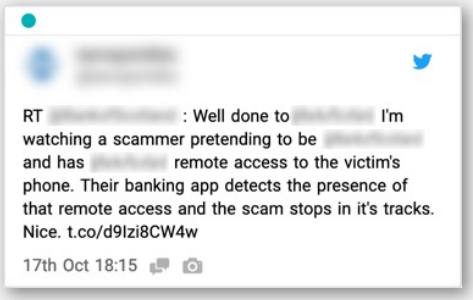
Consumers posted praise when fraud cases were handled quickly and efficiently, sharing positive experiences with the public.



Other positive posts celebrated the quick and efficient handling of fraud cases, and the care that banks had for their customers in these instances. Swift actions to complete refunds were shared online, fostering greater trust and loyalty among customers.

Unique interventions

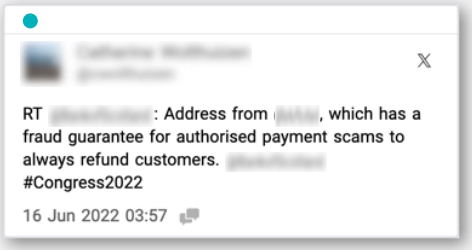
Intervention strategies like fraud hotlines, special security measures and references to new laws and regulations to protect consumers were well received.



Innovative strategies, such as fraud hotlines, enhanced online security features, and personalised customer support were applauded by customers for improving ease and accessibility of fraud reporting.

Accountability

Cases in which banks refunded stolen funds but also acknowledged that fraud had not been detected or were slow to respond were appreciated.

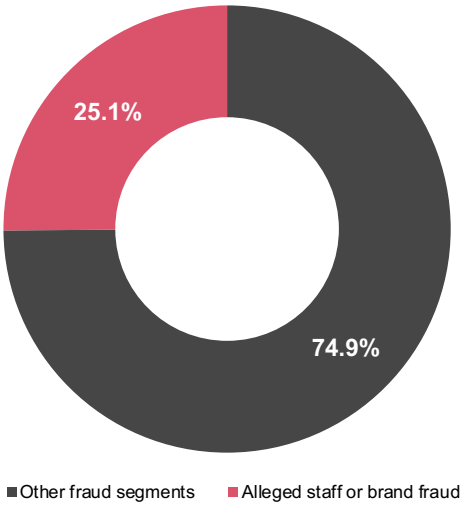


Banks received appreciative feedback when they acknowledged lapses in fraud detection or delayed responses, and compensated customers by refunding stolen funds.

Exploring instances of alleged staff or brand fraud

Allegations of staff-related fraud, unjustified account freezes, involvement in large-scale fraud, and perceived facilitation of fraudulent activities have all been voiced by customers and are notable areas of concern.

Proportion of alleged staff fraud vs. other fraud segments



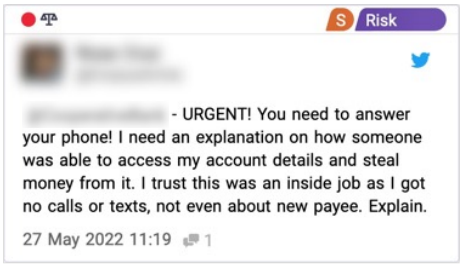
Verified non-enterprise mentions, excluding reshares

Instances in which consumers accused the bank or bank staff of behaving in a fraudulent manner accounted for one-quarter of fraud-related conversations in the banking industry.

Alleged employee-related fraud

25.1% of conversations in this topic alleged staff involvement in instances of fraud, perhaps reemphasising an underlying level of institutional distrust across the sector. Customers accused bank employees of perpetrating fraud citing allegations of mysterious account deductions, unexplained fees, or suspicious staff communications.

Customers often posted about these suspicious communications to warn other customers and asked banks to confirm whether requests were official or not. This highlights the importance of rigorous staff training and clear customer communication protocols.

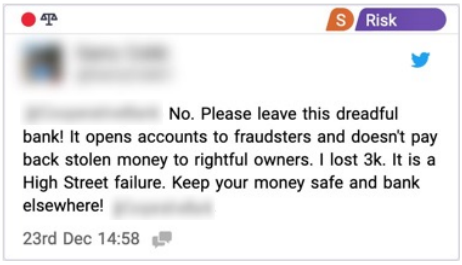


Blocked or frozen accounts

Some customers alleged unjust withholding of funds, which led to accusations of bank fraud when they were unable to access their money, a sensitive issue given anti-money laundering regulations and risk around tipping off. Providing information to staff to allow them to distinguish between reasons for account freezes could help improve customer experience in cases where freezes were initiated to protect customer funds (e.g. account take-over prevention).

Alleged facilitation of fraud by banking processes

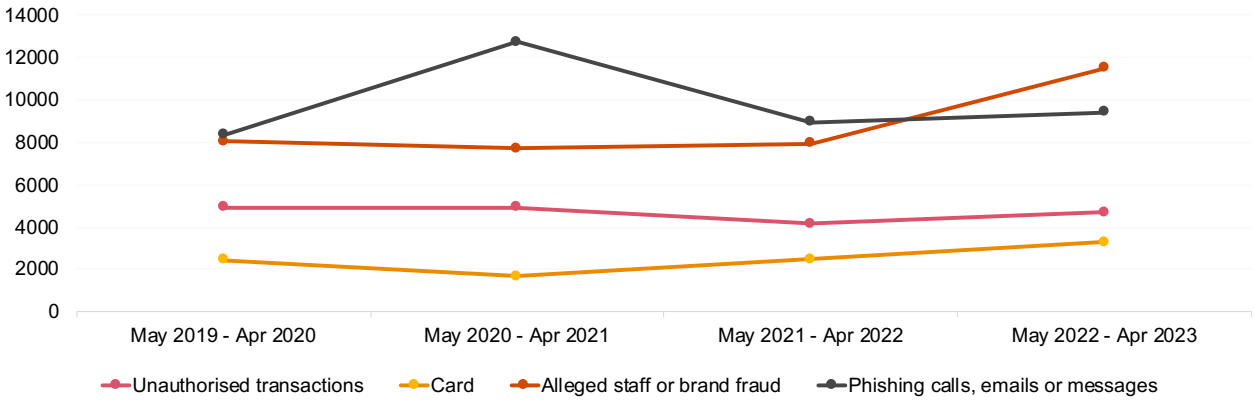
Some banks were accused of enabling fraud by permitting alleged or known fraudsters to maintain accounts containing scammed funds. When banks did not return these funds, it angered consumers and highlighted their expectation that banks should not only actively prevent fraud, but also manage and repair any negative consequences to the best of their abilities. The introduction of reporting requirements on recipients of scam funds as part of the PSR's APP fraud mandatory reimbursement regime will provide new visibility of these kinds of issues and could adversely drive media attention.



Fraud conversation has changed to reflect the evolving threat landscape

As fraud and fraudulent techniques change, so does the related conversation on social media. All types of fraud seem to show a general upwards trend, apart from unauthorised transactions.

Volumes of different types of fraud between 2019 and 2023



Aligned with industry research indicating the level of unauthorised transactions has levelled off or started a downward trend.

Spikes in the data represent scamming trends

The move towards a more digital banking format with additional identity verification security measures means that fraudsters are developing new techniques to gain access to their victims' personal details. Reports of phishing attempts rose, as did reported of attempted hacking and the cloning of cards.

Phishing mentions saw a large spike during the height of lockdown. There is also a noticeable rise in alleged staff or bank fraud starting in April '22.

Unauthorised transactions are declining, but not eliminated

Although conversations around unauthorised transactions have been on a downward trend, they continue to be a significant part of fraud discussions. These conversations were more frequent among digital challenger banks compared to traditional ones, indicating a potentially uneven levels of capability in the detection of suspicious payments.

Digital channels and fraud

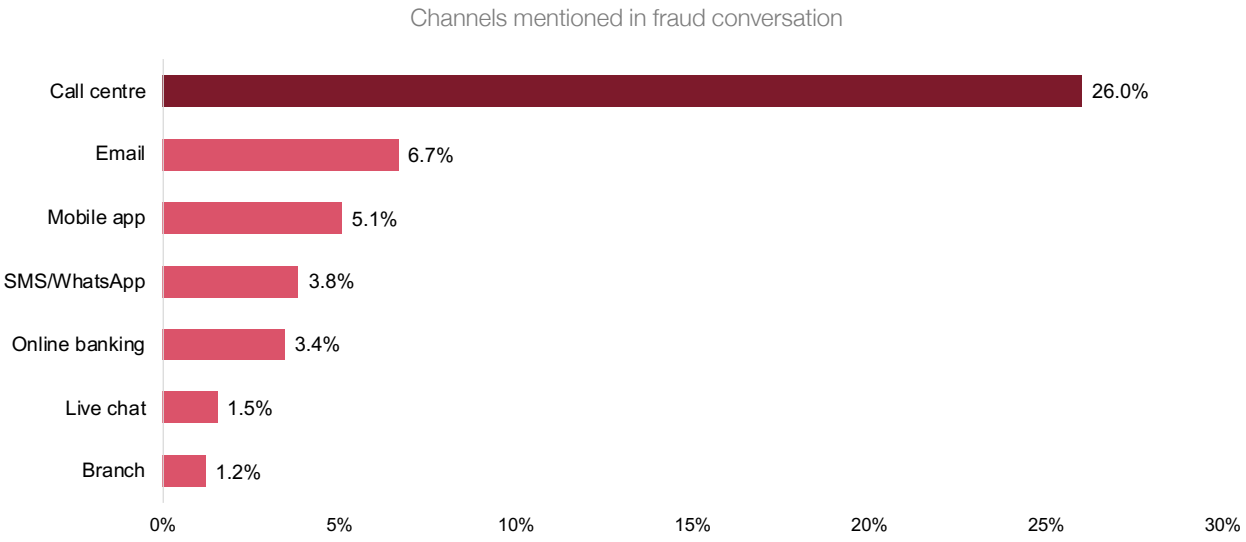
Newer digital challengers seem to experience higher instances of unauthorised transaction discussions than the more established banks. This suggests that the shift towards digital channels might provide increased opportunities for fraudulent activities, highlighting the need for more robust cybersecurity measures.

Technological advancements and cybersecurity

The constant progression of technology fuels the sophistication of criminal entities. Banks face the challenge of keeping their cybersecurity protocols abreast with these advancements, to effectively mitigate the ever-evolving threat landscape.

Call centre challenges indicate the need for varied customer solutions

Call centres emerged as the most commonly mentioned channel for reporting fraud, possibly reflecting customer preference for human interaction, or denoting the severity of the problems faced by customers when dialling into the call centre.



Verified non-enterprise mentions, excluding reshares

Customers often resorted to social media as a last resort after trying multiple channels, including a dead-end or long waits for the call centre. This signals the call centre as a significant hurdle in the fraud reporting process.

	Not getting through at all/ Not getting call back as promised
	Long wait time on hold / in virtual line
	Call dropped when answered or during transfer
	Transferred multiple times or directed to different department / channel
	Unsympathetic / unhelpful staff

Customers frequently complained about unavailability, waiting times exceeding 30 minutes, or calls being dropped abruptly, forcing them to restart the process. Transfers, particularly to the fraud department, were another pain point, often resulting in dropped calls.

Interactions with call centre agents further heightened customers' distress, with reports of staff being perceived as rude, unsympathetic, or lacking knowledge.

These complaints underline the need for operational changes in contact solutions and enhanced training for call centre agents. Providing alternative contact solutions such as 'self-serve' fraud reporting is increasingly becoming standard as banks seek to provide a more automated customer journey and reduce dependency on higher-cost call centres.

4 Servicing fraud reports on social media

Over half of all high-priority mentions did not receive a reply from the bank

Priority mentions are those which posed a potential risk or contained a customer service request, an acquisition opportunity or a cancellation threat. As such, these mentions should be considered as requiring a response from the bank.

43.5% Average response rate

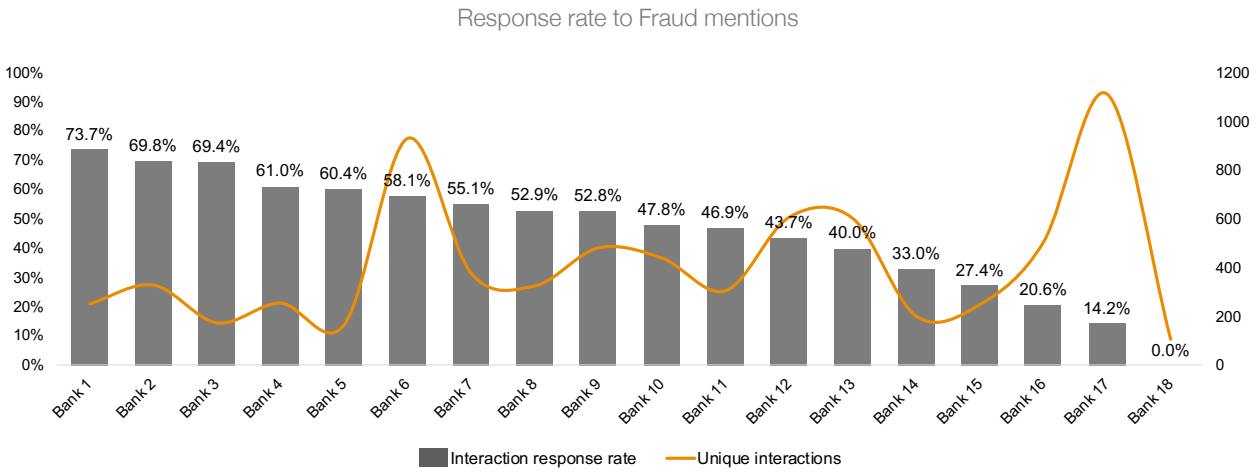
1.9hrs Average response time

The UK banking industry's response rate to priority mentions during the reporting period was 43.5%, which means that over half of all consumers' high-priority mentions went unanswered. For fraud mentions, in particular, this lack of response can be problematic. In some instances when consumers did not receive a reply from the bank, other social media users responded to their posts, with the potential that fraudsters intervene in conversation with false or misleading information.

When banks did respond, their average response time was 1.9 hours. While comparable to other sectors, faster responses might be expected from financial service providers due to the urgency attached to money management.

The banking industry responded to less than half of its fraud interactions

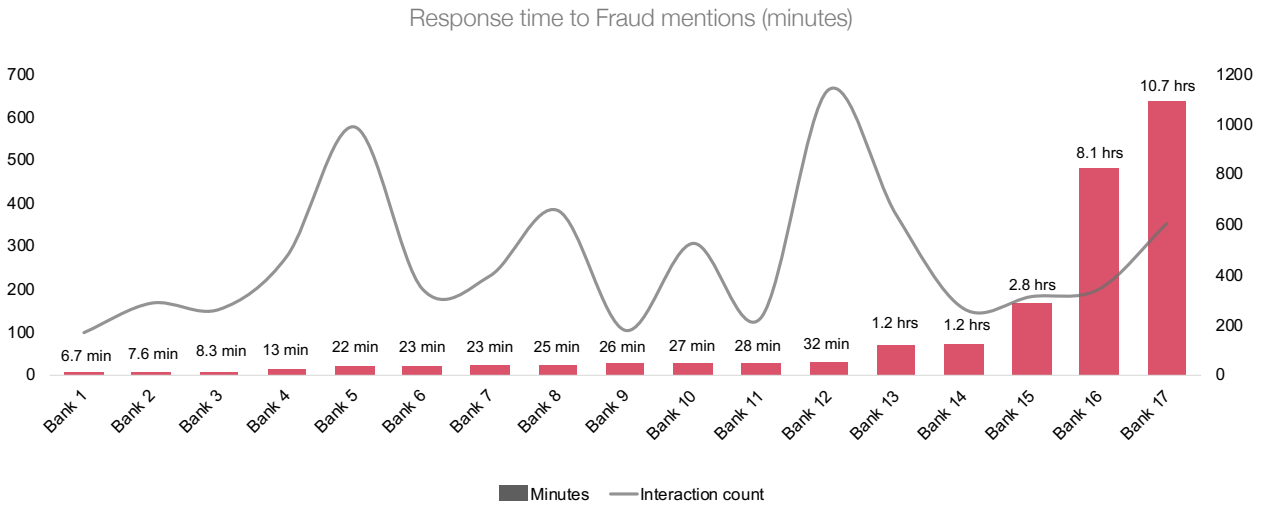
This graph shows the response rate for each bank to fraud-related interactions as depicted by the grey vertical bars. The horizontal yellow line reflects the total volume of fraud interactions per bank.



Non-enterprise mentions, excluding reshares

Most banks took under 30 minutes to reply to fraud mentions

The bars in this graph represent the average response time per brand in minutes. Response time is shown alongside the number of fraud mentions represented by the waving grey line.



Non-enterprise mentions, excluding reshares

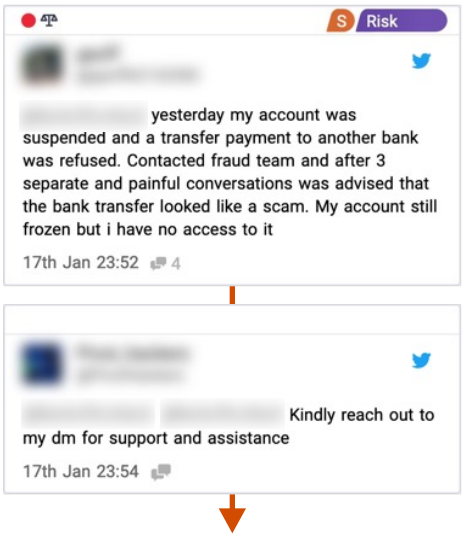
Eleven banks showcased commendable performance, responding to fraud mentions in under half an hour. The leading bank for this metric responded in an average of 6.7 minutes, considerably quicker than the industry average of 67 minutes. This indicates that the leading bank prioritises this type of risk conversation, even though they received one of the lowest rates of fraud-related mentions.

---

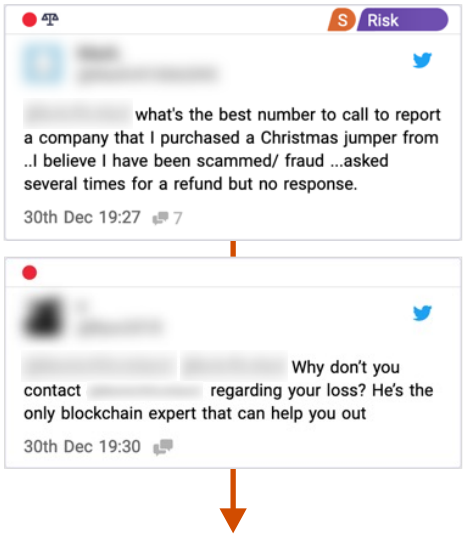
11 of the banks had an average response time of under 30 minutes.

Scammers took advantage of banks' silence

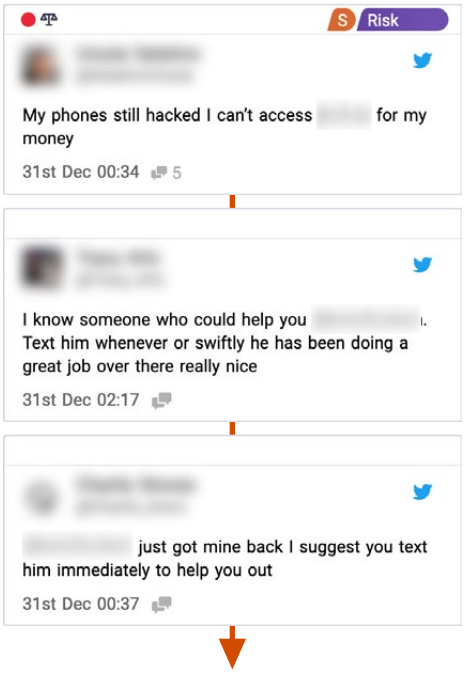
A prompt response from banks is crucial, as silence leaves customers vulnerable to fraudulent exploitation. Scammers can seize opportunities to respond to unresolved tweets with false or misleading information.

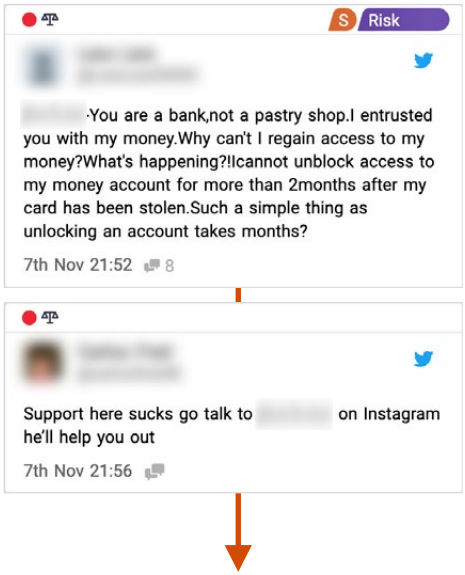


The lack of response from the bank gave potential scammers a window to manipulate vulnerable, confused consumers through coordinated attacks.



In other instances, other users presented themselves as concerned, helpful citizens but there is a risk that these individuals could be scammers. Providing promising solution that many desperate people would jump on, could be an effective strategy for fraudster to engage new victims.





Subsequently, many of the accounts involved in conversations were suspended, and posts were deleted, providing further evidence that they may have related to scammers.

5 Conclusion

Conclusion

This report has highlighted several key insights that shed light on consumer sentiments towards the UK banking sector and the challenges of balancing robust control with customer experience. Social media platforms have emerged as a hub of activity, with customers readily voicing their opinions about their experiences with banks. Analysing these conversations provides a valuable opportunity for banks to better understand their customers' pain points to improve their services and communications, with the potential for ongoing monitoring of sentiment to provide data to enrich understanding of the impact of fraud controls.

The digital banking landscape has grown increasingly varied and complex. While effective fraud prevention measures are a non-negotiable requirement, the consumer's overall experience has emerged as a key differentiating factor.

Evidently, the reputational risk associated with fraud is substantial. Customers are openly expressing their dissatisfaction on social platforms about account blocking, customer service, and inadequate communication during fraud incidents. These experiences can dramatically impact a bank's reputation and customer loyalty.

The banking industry's social media response strategy to these issues can be improved, as indicated by the negative Net Sentiment towards the industry as a whole. More than half of high-priority social media mentions did not receive a response, illustrating an urgent need for improved communication tools and strategies.

Nevertheless, positive examples exist. Certain banks have demonstrated how proactive communication and swift action can effectively mitigate risk, enhance consumer perception, build trust and minimise friction for customers.

Banks can also use automation wisely to improve service delivery and free up agents for moments in a customer's journey, like fraud reporting, where empathy and human understanding are irreplaceable.

The way forward

1. Elevate social media engagement and broaden channels of communication

Timely responses on social media can deter fraudsters and reassure customers. Banks should be actively engaging on these platforms to control the narrative and protect their reputation. Banks should also consider implementing a variety of digital channels to supplement call centres for fraud reporting. Timely and efficient response across all channels is critical to manage and mitigate fraud.

2. Harness technology wisely to optimise the customer experience

Banks can benefit from an improved understanding of the end-to-end customer journey, especially in instances of fraud. Data, including social media feedback, can be leveraged to streamline processes and minimise friction for customers. Banks can also use automation wisely to improve service delivery and free up agents for moments in a customer's journey, like fraud reporting, where empathy and human understanding are irreplaceable.

3. Drive positive sentiment by demonstrating a more proactive response to fraud

Banks should actively communicate about their strengthened security measures, educate the public about fraud prevention, and provide consistent feedback to customer posts. Such actions can foster greater trust and confidence among customers, redefining the narrative to one of the banks and customers uniting against fraud.

Looking forward, the banking sector should consider these key takeaways to exceed customer expectations and improve their industry's sentiment rating. By doing so, they can turn challenges into opportunities, driving customer satisfaction and industry growth.

6 Methodology

Data Collection

DataEQ retrieved 1 768 279 public mentions about 18 major UK banks from Twitter and websites between 1 May 2022 and 30 April 2023. Of these, 1 500 950 were from non-enterprise owned accounts and websites. The original data set was cleaned before sampling to exclude irrelevant mentions.

Sample sentiment for verification

Over 1.5 million public non-enterprise posts were collected between May 2022 - April 2023. To carry out sentiment analysis with a 95% confidence level and an overall 0.1% Margin of Error (MOE), a random sample of 428 081 (28.5%) of these mentions were processed through DataEQ's Crowd for evaluation and verification. Mentions were assigned sentiment scores of positive, negative or neutral.

Risk and Fraud segmentation

All sentiment-verified unique mentions were coded by DataEQ's Crowd for risk tagging. These comprise several operational and reputational themes underpinning banking risk, including discrimination, downtime, protests, health and safety, fraud reports, threats of regulatory action, anti-competitive behaviour, and exploitation. 73 193 mentions in this study contained one or more risk themes.

To deep dive into different types of fraud, DataEQ created a fraud framework and used Crowd verification for thematic tagging on risk mentions. Just over 7 900 mentions contained at least one of the following themes:

- **Brand actions towards fraud**
- **Unauthorised payments or transactions**
- **Password or credential stuffing**
- **Alleged staff or brand fraud**
- **Cyber or digital security**
- **Miscellaneous or other fraud**
- **Phishing emails, calls or messages**
- **Card fraud**
- **Crypto fraud**

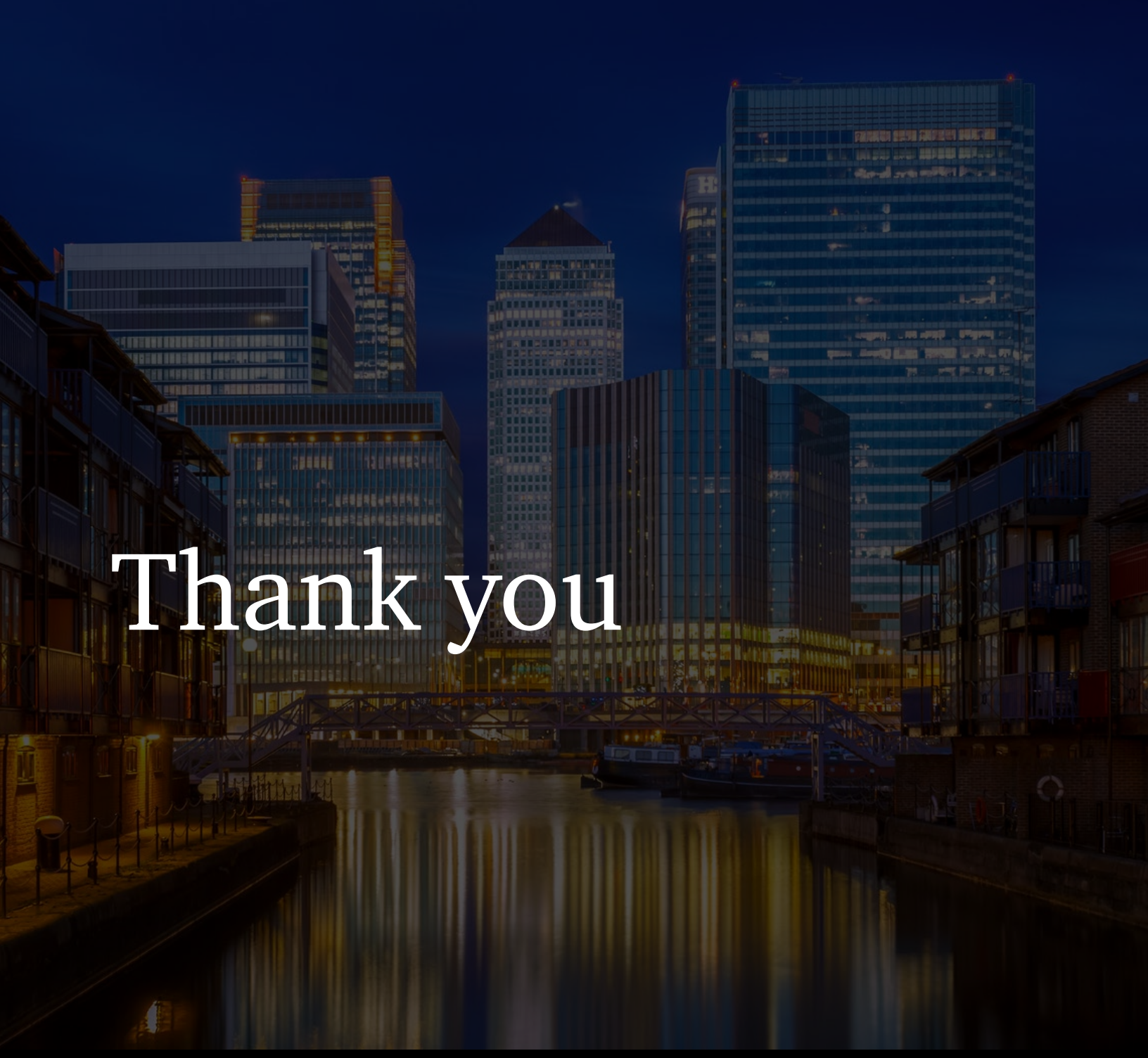
Contacts

Alex West
Director | UK forensics
PwC
alex.e.west@pwc.om

Harry Holdstock
Partner | Financial crime
PwC
harry.g.holdstock@pwc.com

Jamie Botha
Head of partnerships | UK and Middle East region
DataEQ
jamie.botha@dataeq.com

Nadine Whittal
Banking insigths analyst
DataEQ
nadine.whittal@dataeq.com



Thank you

In collaboration with

DataEQ

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2023 PricewaterhouseCoopers LLP. All rights reserved. 'PwC' refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.