The Human Impact of Fraud and Financial Crime on Customer Trust in Banks

feedzai

April 2023

Overview

Who do customers trust more? Their banks? Or a fraudster? It often depends on the messaging — which may give fraudsters an advantage.

If customers are more vulnerable to scams and fraudulent activities than they are to their own bank's attempts to prevent these crimes, it could be because fraudsters' methods or messages connect more with customers than their banks do. In today's rapidly changing financial landscape, it is more important than ever for banks to foster strong relationships with their customers and establish trust. This is especially true as customer loyalty decreases and people become increasingly willing to switch banks. To better understand the public's perception of fraud and financial crime and how their bank works to protect them, Feedzai conducted a comprehensive survey of 4,000 participants in the United States and the United Kingdom.

The survey results revealed that many bank customers are unaware of the distinctions between various types of financial crimes and rely heavily on their banks for reimbursement. In many cases people are lulled into a false sense of security by the numerous, generic warnings that they receive. A significant knowledge gap was also found regarding emerging technologies such as ChatGPT and deepfakes, with 52% of respondents unfamiliar with deepfakes and 63% having never heard of ChatGPT. This raises concerns about the potential for these technologies to be used by fraudsters and underscores the need for greater public education and awareness.

The survey highlights the importance of appropriate customer education and awareness about fraud and financial crime. For example, 77% of respondents indicated that they would leave their bank if they did not receive a refund for a scam, and 53% believe their bank should reimburse them if they are a victim of a scam or third-party fraud. The results also show the potential of AI and other advanced technologies to enhance security measures and better protect customers from these threats, with 53% of customers feeling safer knowing their bank uses AI to protect them.

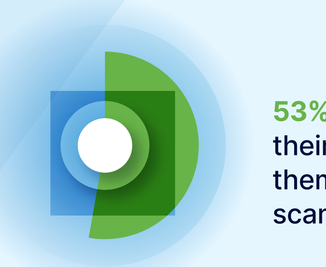
The findings have far-reaching implications in a world where financial institutions face mounting challenges, and consumers are increasingly concerned about failures and costs. As such, banks, governments, and other stakeholders must work together to raise awareness, educate customers about emerging technologies, and promote vigilance in order to mitigate risks and enhance overall security.

Some insights from the survey include:

56% of all respondents said they had been the victim of a financial scam

81%

of respondents would consider leaving their bank if it was publicly fined for failures in anti-money laundering processes



53% of all respondents say their bank should reimburse them if they are a victim of a scam or third-party fraud

53% of customers feel safer knowing their bank uses AI to protect them

77%

of respondents will leave their bank if they do not receive a refund for a scam

Survey Results

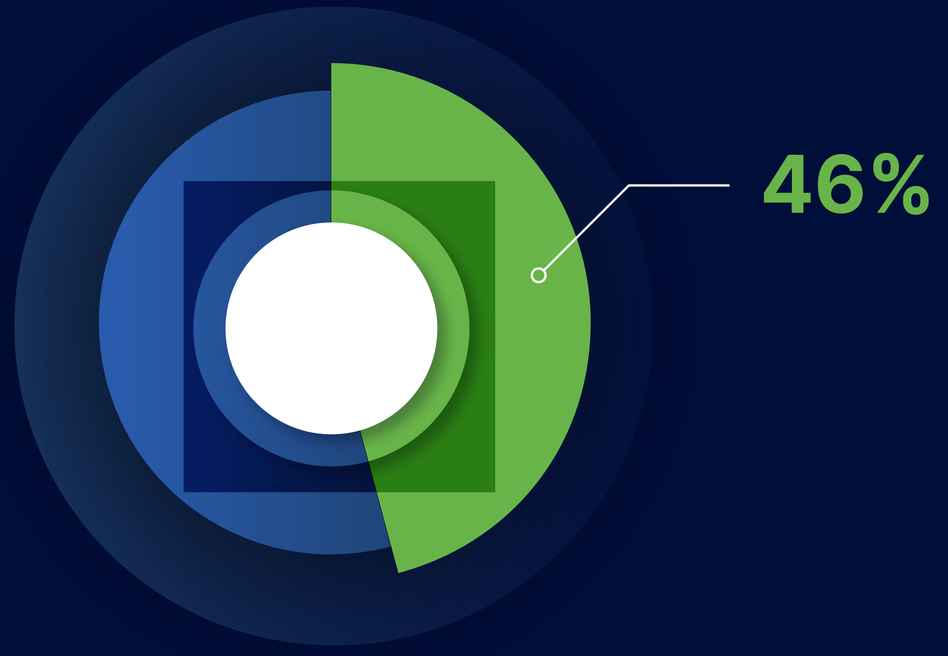
Artificial Intelligence and Customer Loyalty

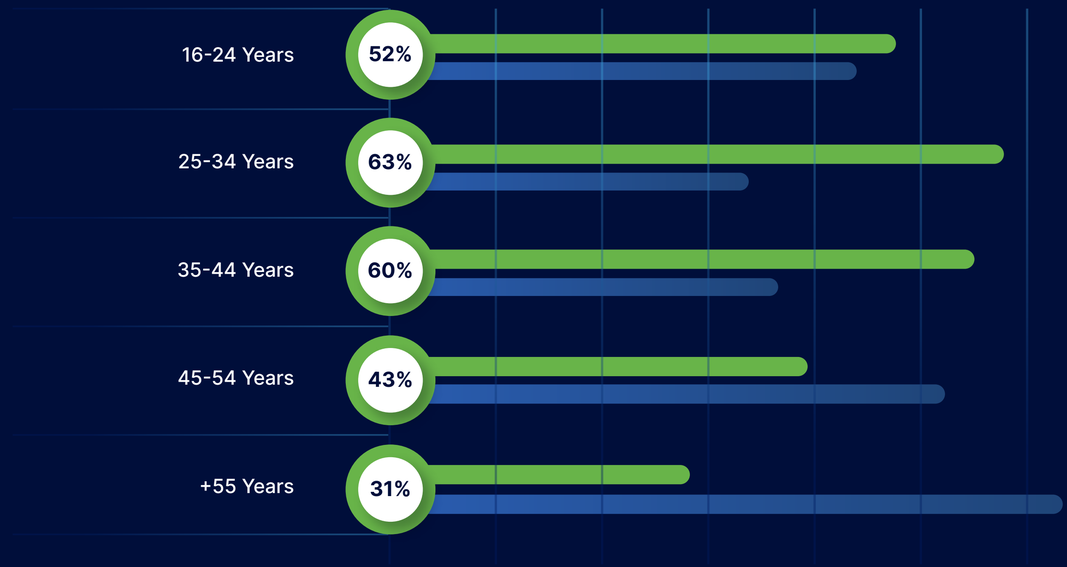
In today's rapidly evolving digital landscape, financial institutions are under increasing pressure to safeguard their customers from financial fraud and money laundering. With the advent of AI technology, financial institutions now leverage advanced machine learning models to detect and prevent fraudulent activities in real-time. However, the question remains: how do customers perceive the use of AI in banking?

In our survey, we asked customers about their thoughts on AI, including how it impacts their feelings of safety, what they believe the future impact of AI will be on financial crime, and how they would react if their bank stopped a legitimate transaction, even if it was quickly resolved. The results are insightful and reveal key insights that financial institutions should consider as they implement AI technology to combat financial fraud and money laundering

46% of all respondents would consider leaving their bank if the bank stopped a legitimate transaction, even if the issue was resolved quickly

The impact of blocking transactions on customer loyalty varies significantly across age groups, but the results of this survey paint a clear picture – transaction blocking can seriously impact customer loyalty, especially among younger customers. Banks need to be careful not to block legitimate transactions, and implement effective safeguards to prevent false positives and avoid customer inconvenience.





81%

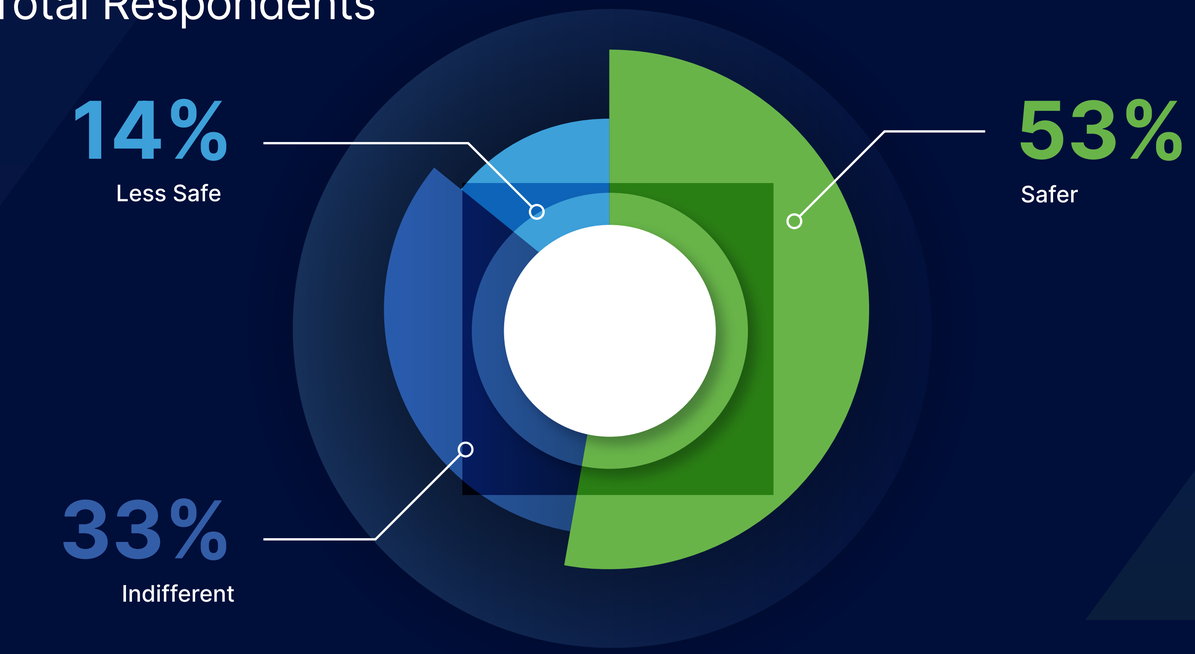
of respondents would consider leaving their bank if it was publicly fined for failures in anti-money laundering processes

These responses are a clear indication that banks need to prioritize AML compliance and take proactive measures to prevent AML failures. To retain customers, banks must have robust AML policies and procedures in place, coupled with effective training programs for their employees.

53% of customers feel safer knowing their bank uses AI to protect them

When it comes to age, younger customers are generally more accepting of AI in fraud prevention, but many still have reservations. Customers 45 and older, on the other hand, tend to feel safer with AI but are still not entirely sold on the concept. Overall, while AI is one of the most powerful tools in the fight against financial fraud, banks must approach its implementation carefully and with full transparency to maintain customer trust and confidence.

Total Respondents



Respondents by age

16-44 Years

59% Safer
30% Indifferent
11% Less Safe

+45 Years

48% Safer
35% Indifferent
17% Less Safe

Customer Sentiment Regarding AI in Banking

When we asked respondents open-ended questions about the likely impact of developments in AI technology for financial crime, five themes emerged:

Awareness of the need to continuously fight fraud

Respondents recognized that preventing fraud is a continuous battle and that criminals are always adapting and finding new ways to scam people.

Fear of abuse and data theft

Some worried about the potential for AI to be hacked or for customers to be exposed to new levels of crime. They suggested that fraudsters would find ways to use AI against security systems.

Limited knowledge and awareness of fraud prevention

There was concern about respondents' limited knowledge and awareness of fraud prevention in general and AI fraud prevention in particular. They wanted more information and education to keep up with new scams and schemes and to make more informed decisions around AI and fraud prevention.

Fraud and Scams

We delve into the increasingly complex world of fraud and scams, focusing on the challenges banks and their customers face in identifying and responding to various types of financial crimes. Our findings reveal that many customers do not differentiate between authorized push payment (APP) scams, account takeover fraud (ATO), and theft and expect their banks to make them whole regardless of the fraud or scam type.

We explore the growing prevalence of imposter and romance scams, which continue to victimize unsuspecting individuals, causing financial loss and significant emotional distress. These scams underscore the importance of raising awareness and equipping customers with the tools to recognize and report such deceptive tactics.

Finally, we address the rising cost of fraud liability and the diverging regulatory landscapes between the UK and the US. In the UK, regulators have mandated banks reimburse customers for online APP fraud, creating a sense of security and trust. Meanwhile, no such regulation exists in the US, leaving customers more vulnerable to the financial repercussions. They are also much less inclined to report scams or report them as unauthorized fraud. This makes it much harder to accurately measure the full extent of the problem and, more importantly, build defenses to better protect victims.

77%

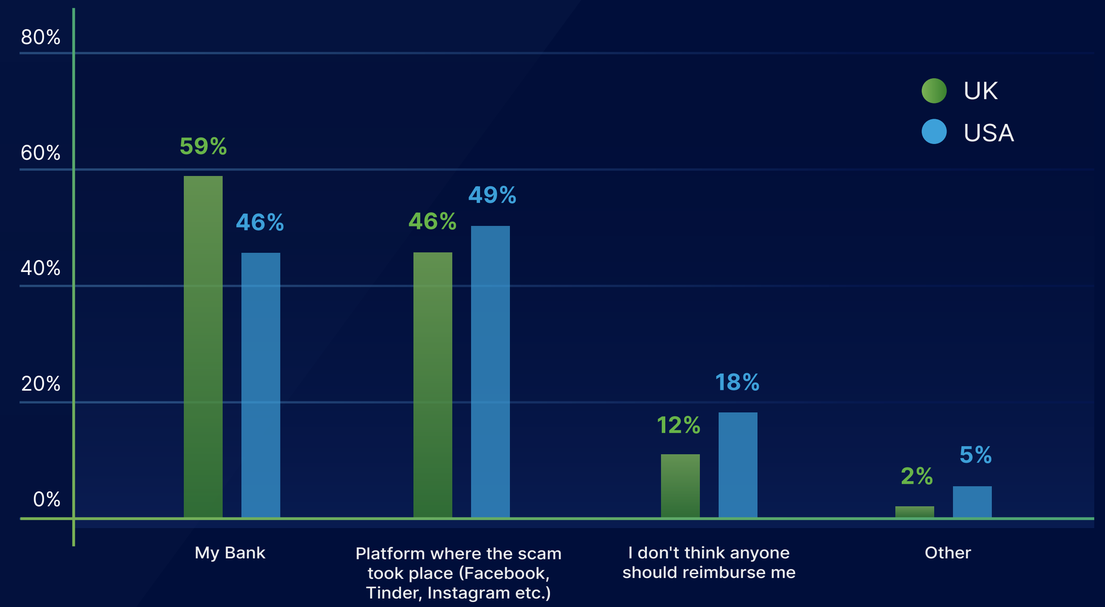
of respondents will leave their bank if they do not get a refund for a scam

Respondents do not make distinctions between APP fraud and ATO attacks, particularly in the US. This may illustrate that more customer education is required. It also highlights the importance of customer trust and satisfaction in maintaining long-term relationships and loyalty in the competitive financial services landscape.

53% of all respondents say their bank should reimburse them if they are a victim of a scam or third-party fraud

Who do you think should reimburse you when you become the victim of a scam via a third party, if anyone?

Breakdown by Country



These recorded differences between US and UK answers may be influenced by the UK's voluntary Contingent Reimbursement Model Code for UK banks. This demonstrates that both united industry and regulatory action can shape customer expectations and increase trust in the financial sector.

79%

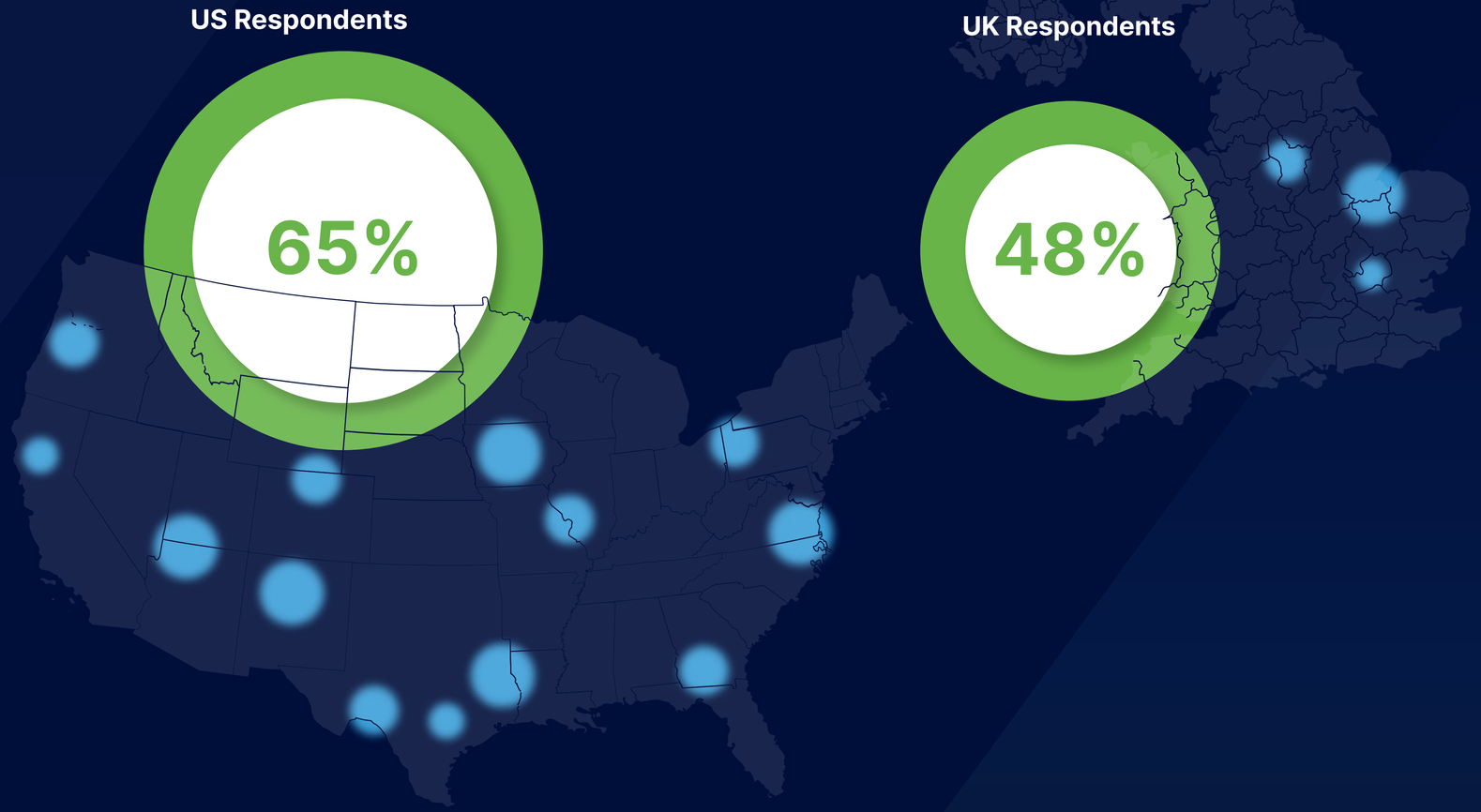
of respondents ages 25 to 44 will leave their bank if it blocks a legitimate transaction, even if the matter is quickly resolved

This result underscores the importance of balancing security measures with a seamless customer experience, particularly for this age group. As practical digital natives, these customers have come to expect both convenience and efficiency in their banking interactions, making them less tolerant of disruptions, even those intended to protect their accounts.

56% of all respondents said they had been the victim of a financial scam

More than half of the consumers surveyed have experienced fraud. This underscores the importance for banks to prioritize fraud prevention and customer education in their strategic initiatives.

US respondents experienced considerably higher fraud rates than the rates reported by banks, which implies that customers are not reporting scams to their banks. While UK respondents reported lower rates, 48% is still a substantial figure.



#1 Channel for US Scams is Social Media

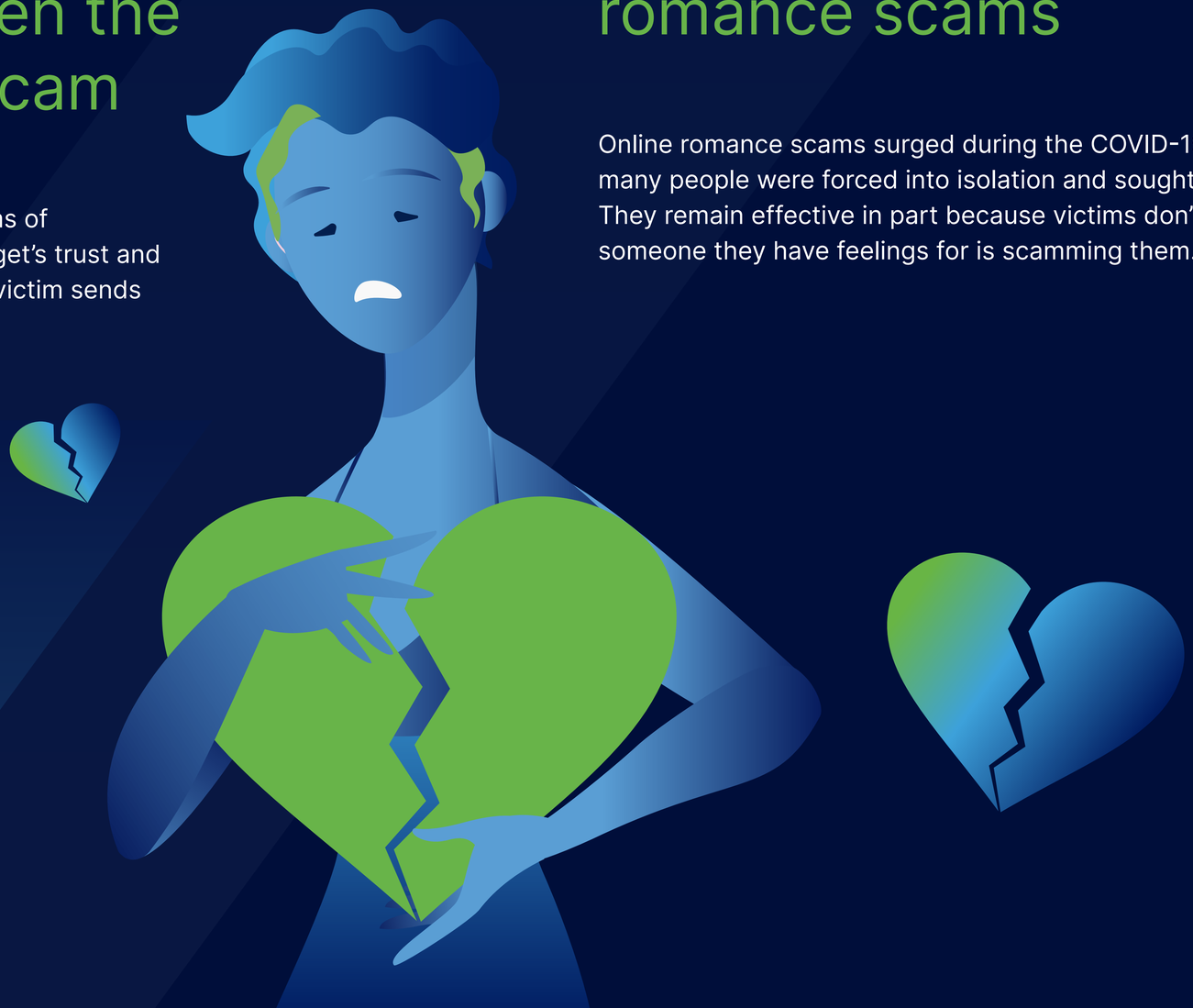
For US survey respondents, social media was the top-ranked contact method used by scammers. For UK survey respondents, social media, email, and phone were all ranked equally as contact methods used by scammers. This demonstrates that UK customers face a more evenly distributed risk across various channels. These findings underscore the importance of adopting a comprehensive approach to customer education, covering all three communication methods and emphasizing the need for vigilance in every aspect of customers' digital lives.

36% of respondents either have been, or know someone who has been the victim of a romance scam

Romance scams are arguably one of the cruelest forms of consumer-facing fraud. Scammers first build their target's trust and then ask them for money for travel or gifts. Once the victim sends money, the scammer ghosts them.

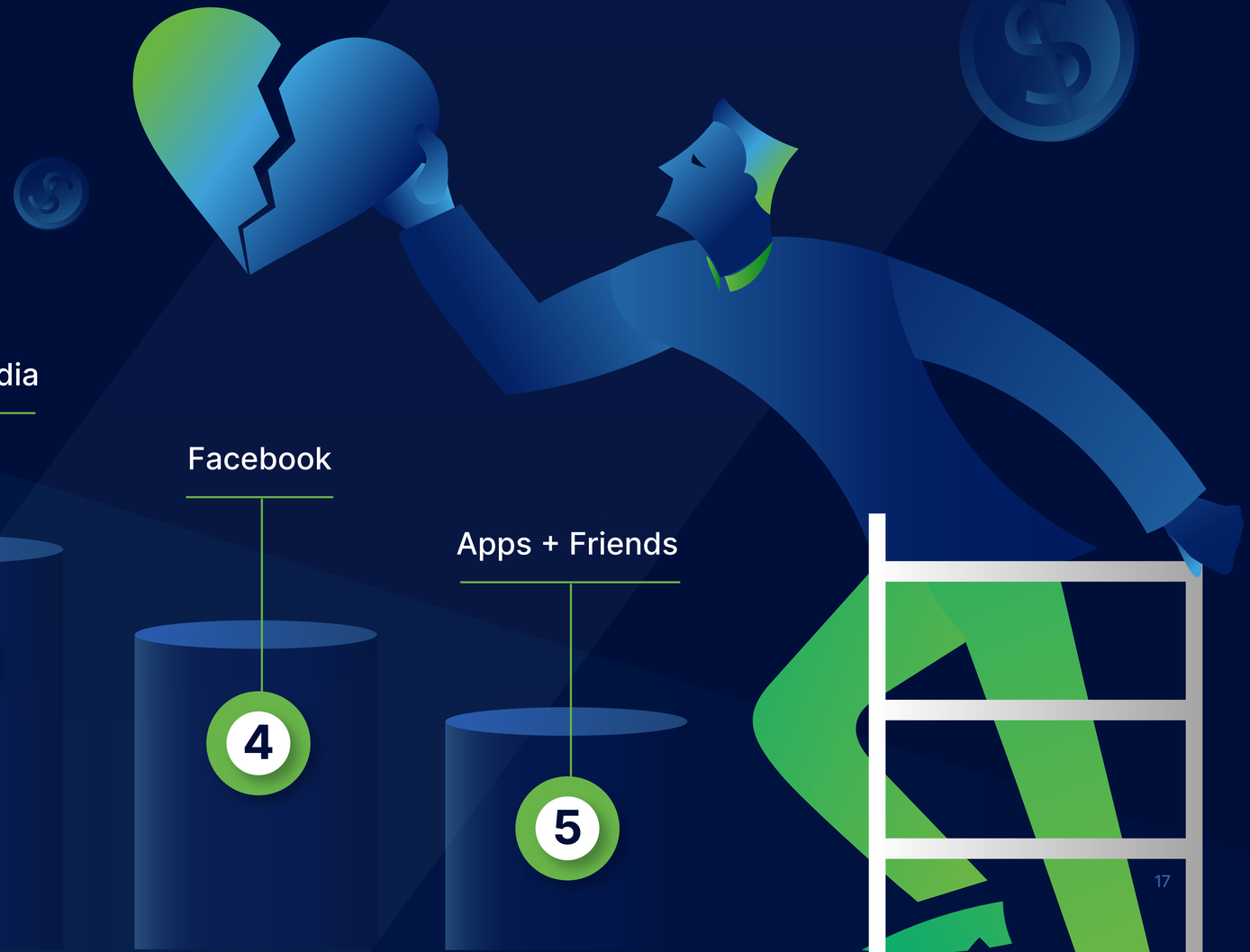
13% of respondents lost more than $8,400 to romance scams

Online romance scams surged during the COVID-19 pandemic when many people were forced into isolation and sought connections. They remain effective in part because victims don't want to believe someone they have feelings for is scamming them.



#1 Source of Romance Scams are Dating Apps and Sites

In an open text answer, respondents who were victims of romance scams ranked the original contact point as:



1. Dating apps or websites
2. Online
3. Social Media
4. Facebook
5. Apps + Friends

5 Signs To Help Consumers Spot a Romance Scam

The person seems too good to be true

They're incredibly attractive? They're successful? They're rich? Chances are if something (or someone) seems too good to be true, they are. Don't immediately fall for outward appearances and sparkle.

They say the 'L' word fast

Scammers need their victims to stay engaged in order to trick them and many declare their "love" early in the hopes of keeping victims engaged.

They ask for money

A common tactic is for the scammer to ask for money for a personal, family, or medical emergency. Others say they need money to travel to meet in person.

They don't want to be seen

Scammers often have an excuse to avoid meeting in person or appearing on camera, such as working in the military or overseas.

Incomplete or inconsistent profiles

Some scammers use fake or stolen information to build an online profile. In some cases, their profile may contain inconsistencies or vague details meaning their stories don't make sense.

4 Ways Banks Can Help Romance Scam Victims

Romance scam victims often feel ashamed and embarrassed about falling for the scam, making them hesitant to report it or seek help. Here's what banks can do to support romance scam victims and protect other customers from falling for similar scams.

Educate customers

Teach customers how to recognize the signs of scams so they can protect themselves.

Create a digital reporting form

Offering customers a digital option to report scams (including screenshots and contact information) without having to discuss their ordeal with another person may encourage more victims to come forward.

Know your users and watch for unusual behavior

Understanding your customers' typical patterns can help your bank identify suspicious behavior and block risky transfers.

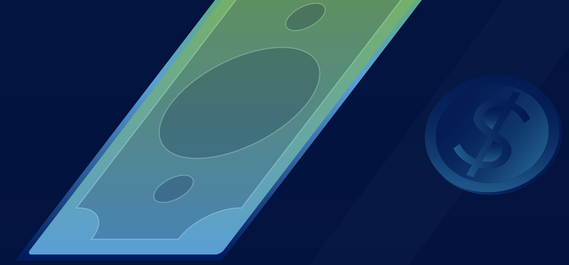
Provide resources

Banks should offer emotional support and counseling to help victims process their experience and help them move forward.

Money Mules

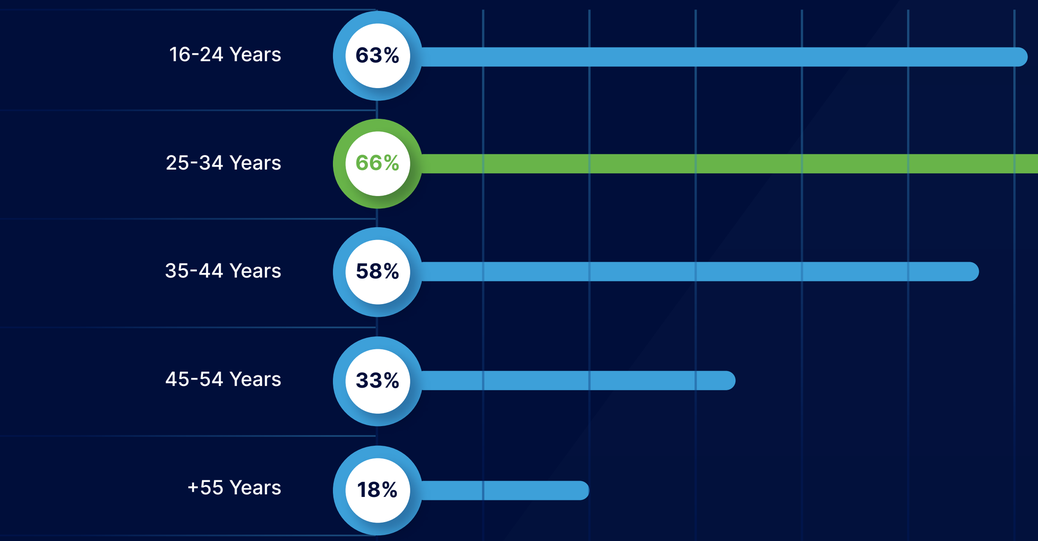
With a surge in digital banking services and an ongoing cost of living crisis, money mules have become an increasingly prominent aspect of cybercriminals' economic business models. Money mules are individuals whose bank accounts are used by fraudsters to receive and transfer illicit funds, ultimately aiding in the proliferation of scams and money laundering activities. In this section of our report, we delve into the disturbing world of money mules, both the unwitting and witting accomplices who play a pivotal role in the ever-evolving landscape of online fraud.

Our analysis sheds light on the demographics of those targeted to become money mules, examining factors such as age, sex, and geographic location. Additionally, we explore the various channels and platforms where fraudsters are most likely to recruit potential money mules. By uncovering these trends, we aim to equip fraud and anti-money laundering leaders with valuable insights into the tactics and methods employed by cybercriminals, thereby empowering financial institutions to better protect themselves and their customers against this insidious threat.

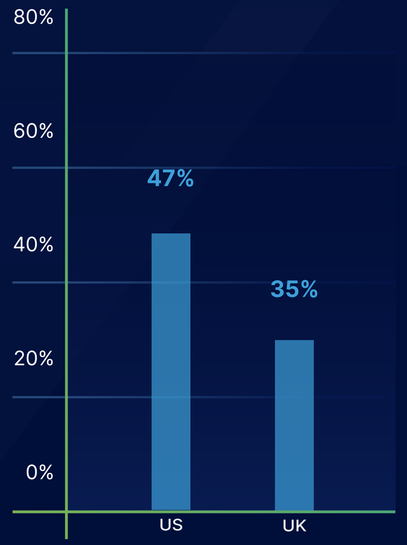


66% of all respondents aged 25-34 are targeted as money mules

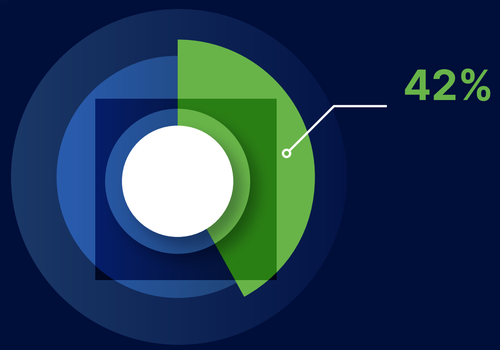
While the survey found consumers aged 25-34 to be the most recruited, all groups under 44 were heavily enlisted.



Respondents asked to receive funds



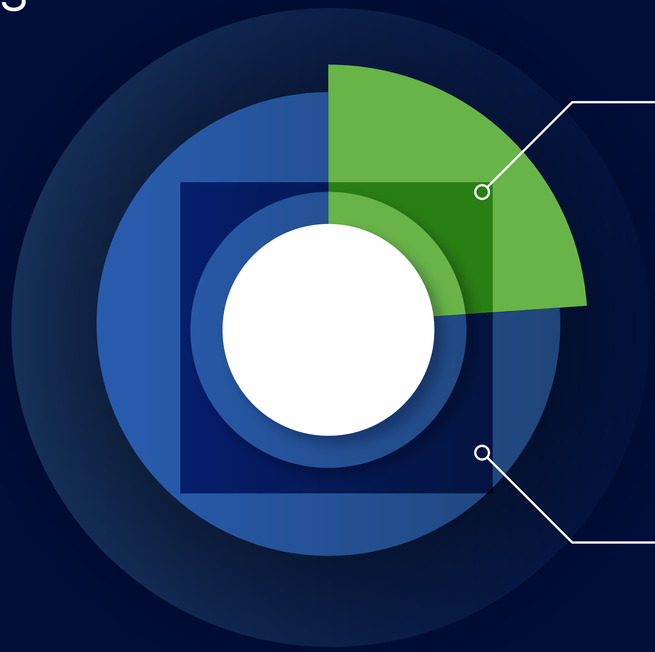
All Respondents approached on social media to become money mules



These results provide valuable insights into how criminals target and recruit everyday people into acting as money mules. Banks can use this information to target outreach campaigns to high-risk customers.

Consumers unaware of the risks of being a money mule

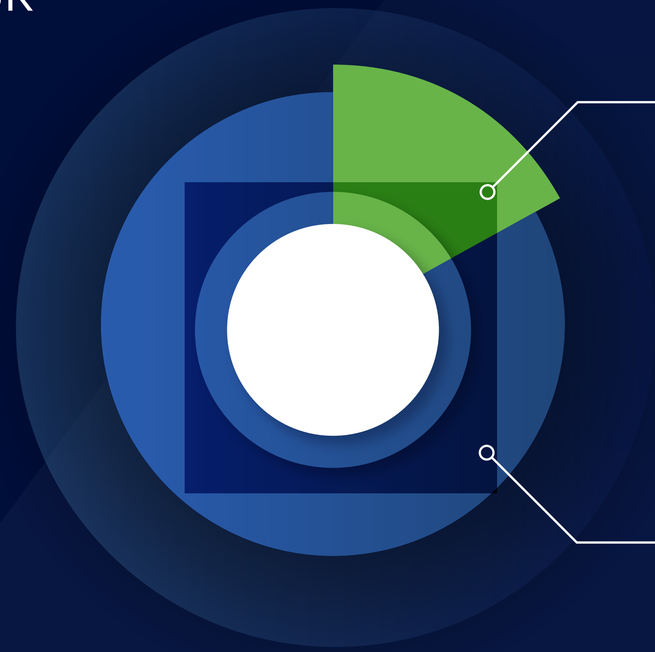
US



24%
Unaware

76%
Aware

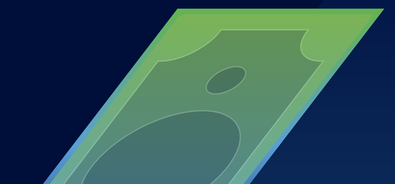
UK



17%
Unaware

83%
Aware

Learning that 80% of all respondents are somewhat aware of the risks of being a money mule is encouraging. However, a lack of awareness by almost a quarter of the US population and 17% of the UK population leaves plenty of individuals vulnerable to exploitation by criminals.



3 Essential Tips for Consumers to Combat Money Mules

Be cautious of unsolicited offers

If someone approaches you on social media or through any other channel with a proposal to provide a service for a small fee, it's best to ignore them.

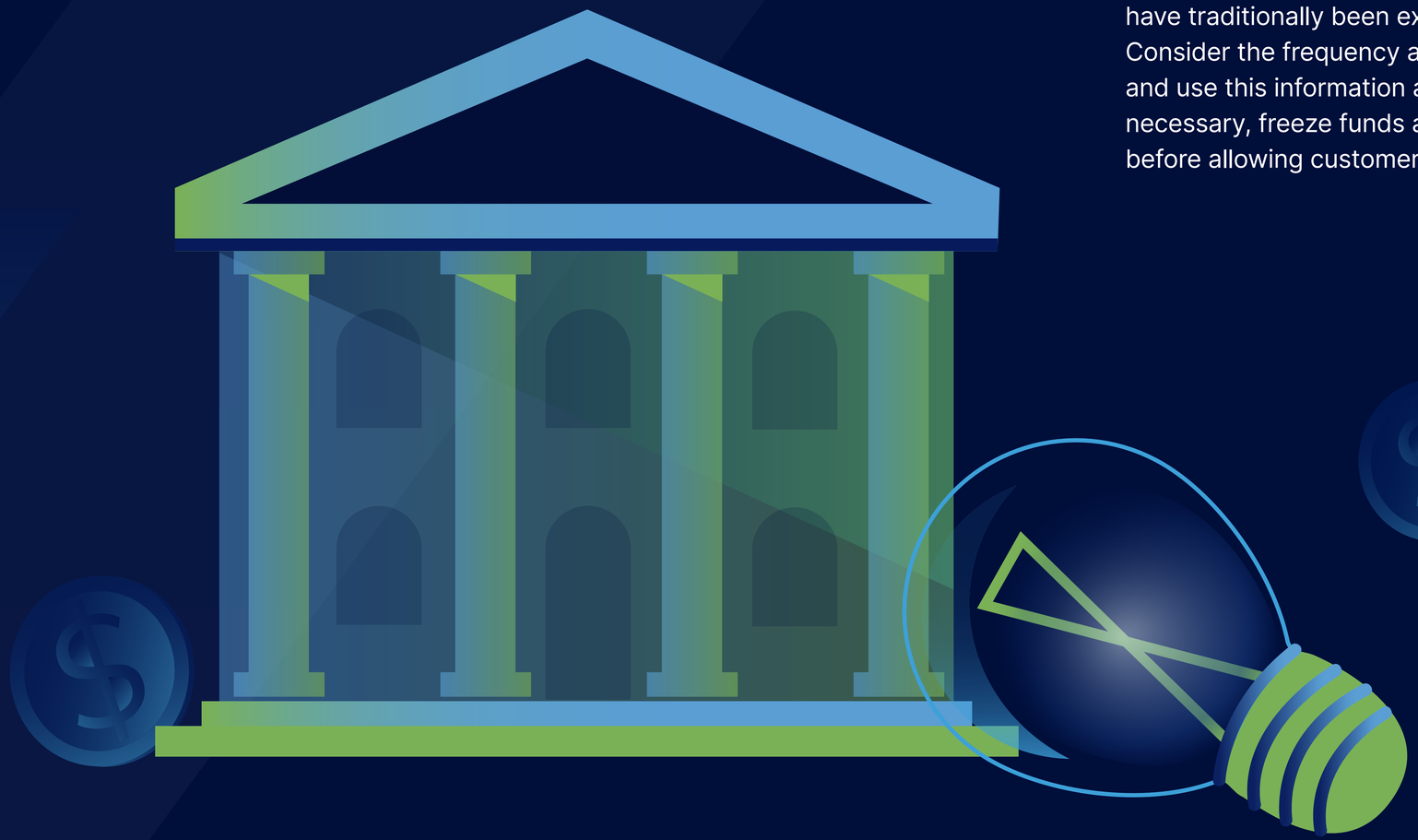
Safeguard your bank account access

Never grant someone you don't know or trust access to your bank accounts.

Protect your financial information

Refrain from sharing your details with people you don't know or trust.

2 Strategies Banks Can Implement to Tackle Money Mule Challenges



Monitor lifecycle risk propensity

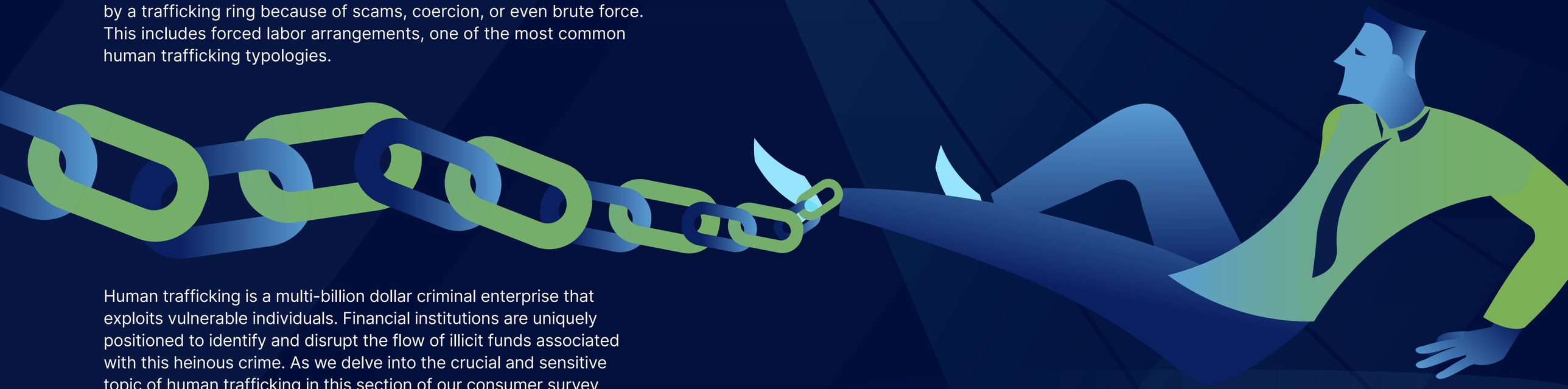
Banks should analytically identify subtle changes in account behavior or how customers interact with their accounts. Any deviations can serve as red flags for further investigation.

Scrutinize inbound payment transactions

Examine inbound transactions as closely as outbound transactions have traditionally been examined, but with a focus on fraud detection. Consider the frequency and typical amounts of incoming transactions, and use this information as a baseline to identify anomalies. When necessary, freeze funds and verify the intention behind deposits before allowing customers to access them.

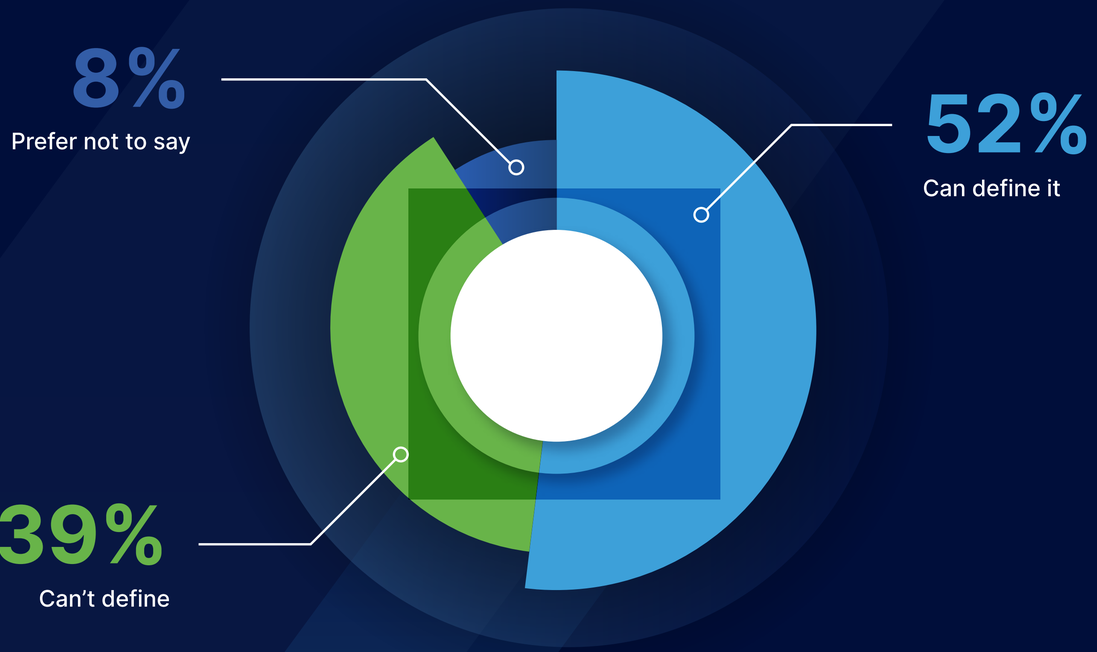
Human Trafficking

It's easy to hear the term "human trafficking" and think of adults or even children forced into the sex trade, but human trafficking is so much more than that. Every day, people can find themselves trapped by a trafficking ring because of scams, coercion, or even brute force. This includes forced labor arrangements, one of the most common human trafficking typologies.

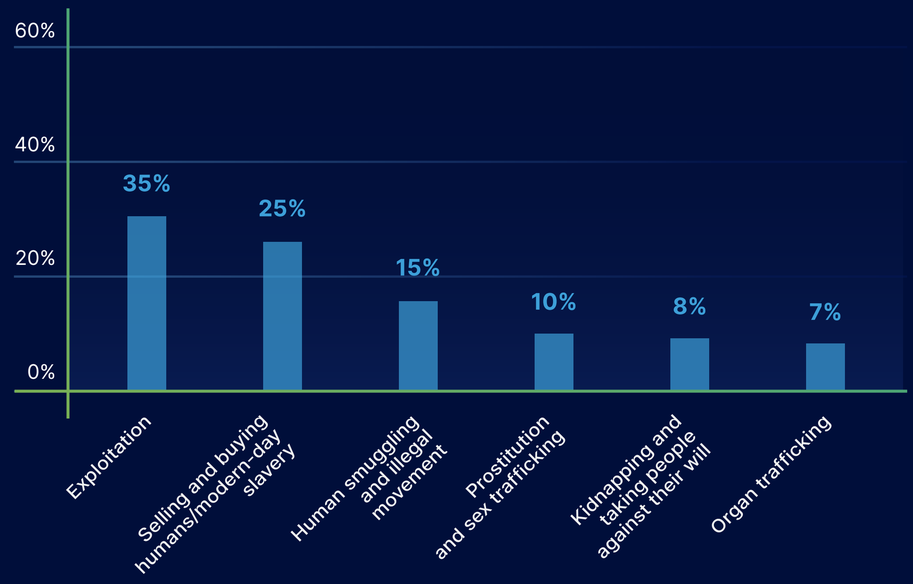


Human trafficking is a multi-billion dollar criminal enterprise that exploits vulnerable individuals. Financial institutions are uniquely positioned to identify and disrupt the flow of illicit funds associated with this heinous crime. As we delve into the crucial and sensitive topic of human trafficking in this section of our consumer survey report, we shed light on banks' critical role in detecting and mitigating this global scourge. Through our analysis, we aim to equip banks with valuable insights into consumer perspectives and behaviors, enabling them to strengthen their anti-human trafficking efforts and better safeguard their customers from inadvertently participating in or facilitating such activities.

39% of respondents can't define 'human trafficking'



52% of respondents who could define human trafficking categorized it as follows:



These findings highlight a significant obstacle for banks in their efforts to stop human trafficking and its related crimes.

64% believe social media is one of the biggest platforms used for human trafficking

This sentiment is shared across all respondents' geographic and age demographics. And they're not wrong. Polaris, a non-profit organization that works to help victims of human trafficking and forced labor, notes that social media platforms, including Facebook, Instagram, WhatsApp, SnapChat, and dating apps like Tinder and Grindr, are often cited as the source of human trafficking recruitment.

85% believe social media companies should do more to stop human trafficking on their platforms

These results highlight the urgent need for collaboration between financial institutions and social media platforms. It is difficult for social media to act without the all-important feedback of fraud outcomes that the banks have. The information is available. What is lacking is the regulatory regime that allows the two industries to work together. By doing so they can develop strategies to identify and counteract human trafficking activities, ultimately disrupting the criminal networks exploiting these digital channels.

80%

of respondents are unsure about AI's role in tackling human trafficking

These results are an opportunity for banks to educate their customers and the broader public on the potential of AI-driven solutions in identifying and disrupting human trafficking networks, thereby showcasing their commitment to leveraging advanced technology in combating this pressing issue.

20% of respondents provided open-text responses on AI's role in stopping human trafficking.

The responses generally fell into six different categories:

Positive impact and support

Respondents expressed optimism about AI's role in thwarting human trafficking. They felt confident that AI and advanced algorithms could quickly track keywords and phrases on social media to identify red flags.

AI impersonation and deception

Some respondents believe that AI could be used to catch criminals by pretending to be real victims on social media.

AI targeting vulnerable individuals

Some respondents believe AI can be used maliciously to target vulnerable individuals by befriending them and making false promises.

Facial recognition and location tracking

Respondents believe facial recognition and location tracking technologies can detect the movement of people and traffickers.

Privacy and ethical concerns

Other respondents believe AI can detect messages about human trafficking – but raise questions about if AI can be misused to compromise privacy.

AI limitations and skepticism

Some respondents were skeptical that AI can stop human trafficking.

3 Ways Everyone Can Help Stop Human Trafficking

Educate yourself

You can help combat human trafficking by educating yourself and others about the issue. Share information through social media, participate in local awareness campaigns, or host community events to help spread the word and increase public understanding of the signs and indicators of human trafficking.

Report suspicious activity

If you suspect human trafficking or encounter suspicious activities, report it to local authorities or national hotlines. Reporting such incidents enables law enforcement agencies to investigate and potentially rescue victims. In the United States, individuals can contact the National Human Trafficking Hotline at 1-888-373-7888. In the UK, individuals can contact Crimestoppers at 0800 555 111.

Support organizations fighting human trafficking

Support and volunteer for organizations that combat human trafficking. These organizations often rely on donations and volunteer efforts to raise awareness, support victims, and advocate for stronger anti-trafficking laws and policies. Contributing time or resources to these organizations can amplify their impact.

6 Ways Banks Can Combat Human Trafficking

Analyze transactional geography

Monitor customers' transaction patterns and locations to identify unusual behavior that could indicate potential involvement in human trafficking.

Scrutinize spending patterns

Monitor customers' purchases, such as frequent fast-food transactions, motel stays, or unusual items, which may signal potential human trafficking activity.

Cross-reference customer behavior

Compare customers' recent activities with their expected behavior based on their KYC/CDD profiles to identify inconsistencies that may warrant further investigation.

Utilize databases on human trafficking

Train bank staff to review third-party databases containing information on known human trafficking perpetrators and victims and to recognize connections between customers and these individuals.

Educate staff to spot trafficking signs

Train bank personnel to identify telltale signs of human trafficking, such as suspicious body language, when customers visit the branch in person.

Strengthen onboarding and monitoring processes

Collect comprehensive data on customers during onboarding and adopt perpetual Know Your Customer (pKYC) practices to continuously monitor risk levels and promptly investigate changes in customer behavior.

Emerging Threats: Generative AI

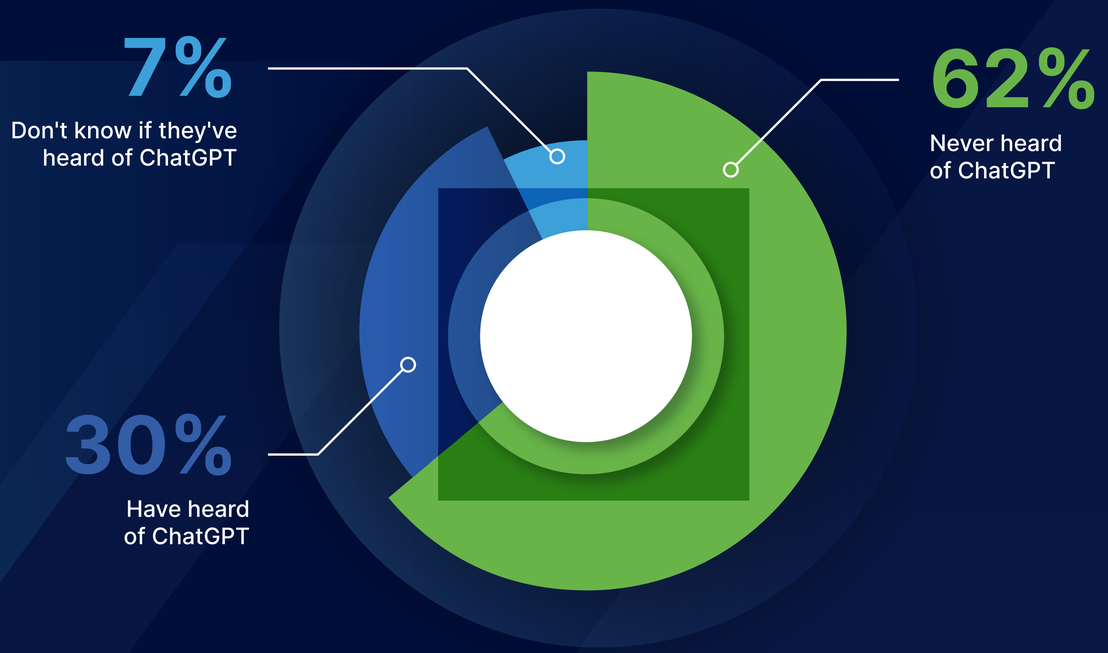
As machine learning and artificial intelligence capabilities continue to expand, so do the potential risks and opportunities for financial institutions. One area of particular concern is the possible exploitation of generative AI, particularly deepfakes and ChatGPT. While these technologies can potentially revolutionize industries from entertainment to healthcare, they pose significant financial fraud and money laundering risks.

Deepfakes, a term derived from "deep learning" and "fake," refer to artificial intelligence-generated media, typically videos, that convincingly replace or manipulate a person's appearance and/or voice. The rapid advancement of deepfake technology raises significant concerns for fraud and anti-money laundering (AML) teams as it becomes increasingly difficult to distinguish between real and synthetic media. Similarly, ChatGPT is a language-processing AI that can generate realistic-sounding text. This technology can create convincing phishing scams or other fraudulent communication that could trick customers and staff.

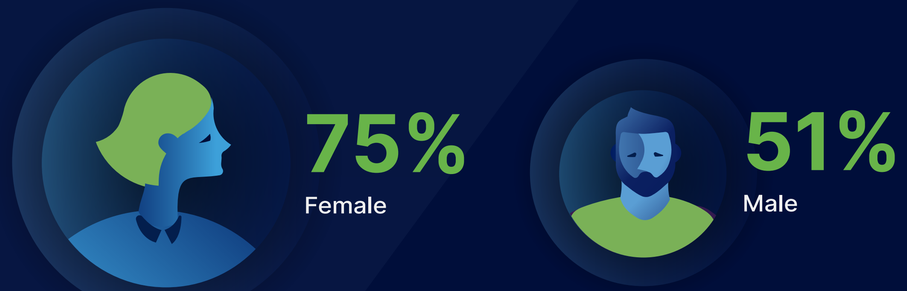
Generative AI will lead to more authorized and unauthorized fraud attacks. Our survey data highlights a critical learning: now, *right now*, is the time to educate customers about deepfakes and to develop the frameworks to combat the coming wave of fraud and financial crime. Banks can protect themselves and their customers from harm by understanding the potential risks of generative AI and developing effective strategies for mitigating those risks.

62% of all respondents have never heard of ChatGPT

These findings highlight a major issue in terms of public awareness and education surrounding emerging AI technologies and their potential uses for fraud and financial crime. It also suggests that a large percentage of the population may be vulnerable to attacks that utilize ChatGPT.



75% of females vs. 51% of males have never heard of ChatGPT



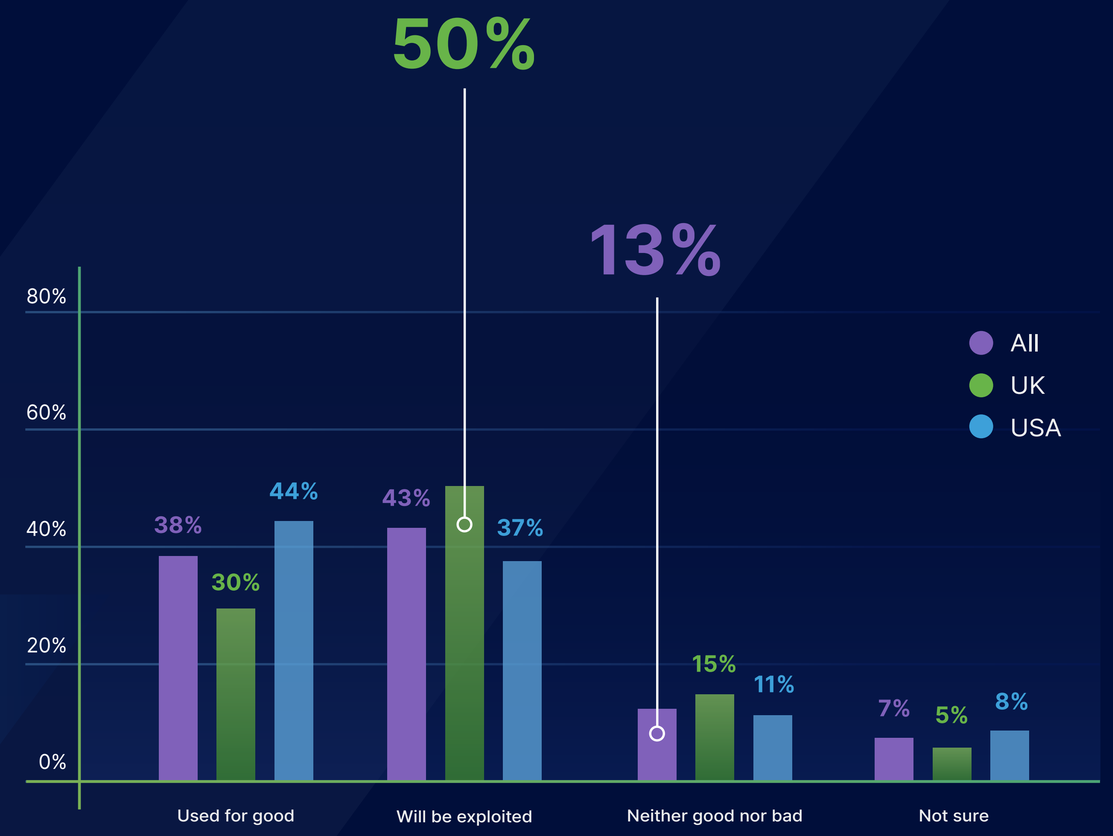
There is a gender divide in terms of awareness of ChatGPT. This may indicate a need for targeted education and awareness campaigns that are tailored to specific demographics.

50% of UK respondents believe ChatGPT will be exploited

When respondents learned about ChatGPT, they were more concerned about it being abused than its potential benefits. There was a significant difference of opinion regarding the potential use of ChatGPT for good or bad actions.

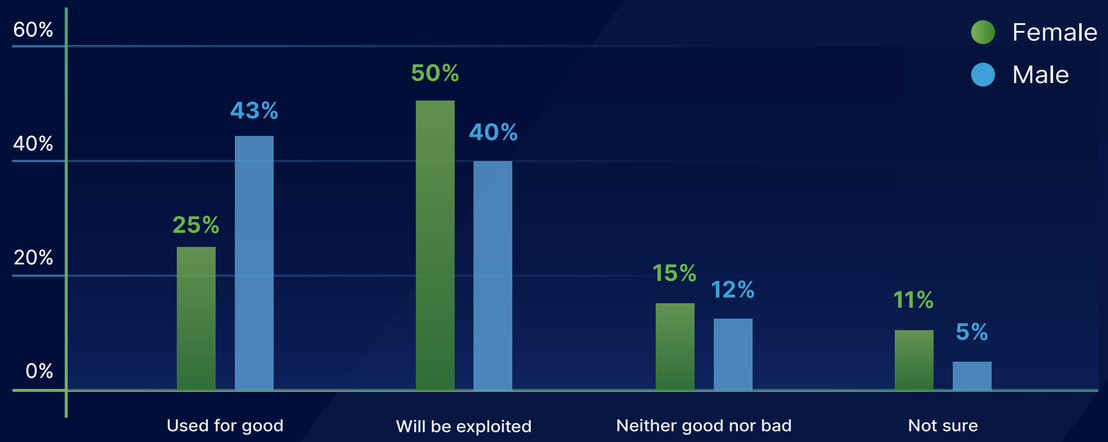
13% of respondents feel that ChatGPT will neither be used for good nor bad actions.

This result may indicate a lack of understanding of the technology, or a sense of ambiguity about its potential uses.



50% of women believe ChatGPT will be used for bad actions

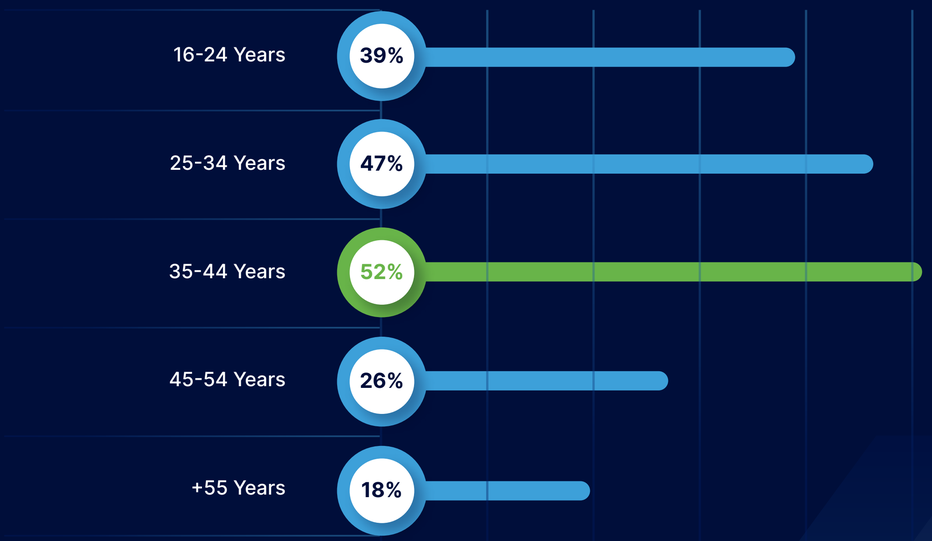
Men and women feel differently about ChatGPT, with men being considerably more optimistic.



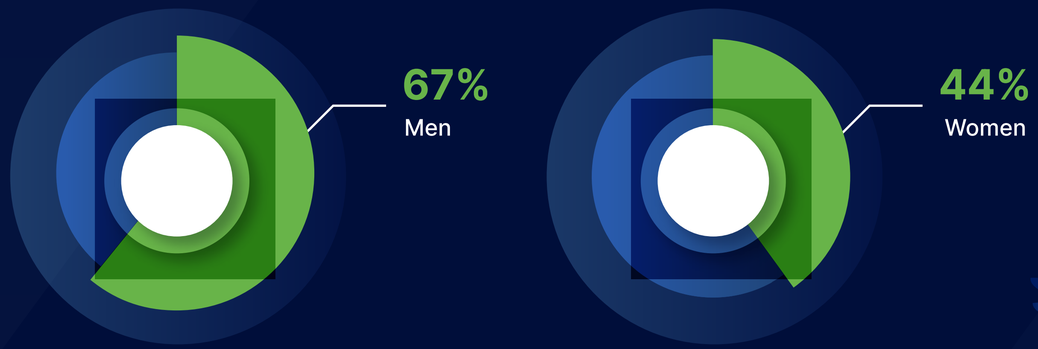
The data shows that men are more likely to believe that ChatGPT will be used for good, while women are more likely to believe that it will be used for bad actions. However, a higher percentage of women are unsure of how ChatGPT will be used. This gender disparity may suggest that men are more familiar with the potential benefits of AI technologies like ChatGPT, while women are more aware of the potential risks and concerns.

52% of 35 - 44 year olds are the most optimistic about ChatGPT

Older consumers are much less likely to hold optimistic views about ChatGPT's potential than younger ones. At the same time, a slim majority of consumers ages 35 to 44 believe the technology can be used for good.



Confidence in spotting an email written with ChatGPT's help



There is a gender gap in confidence to spot emails written by ChatGPT. While two-thirds of men who have heard of ChatGPT are confident in their ability to identify an email written by the AI technology, only 44% of women share that confidence. This could be attributed to differences in technology usage or awareness, as well as variances in individual experience with fraud attempts.

Regardless of confidence levels, the truth is that as this technology evolves, we'll need to use AI to tell us when we're reading something AI generates. Let that sink in.

52% of all respondents don’t know what are deepfake videos

More than half of the respondents were unfamiliar with deepfakes, which is a concerning finding given the growing prevalence of these videos in online spaces.

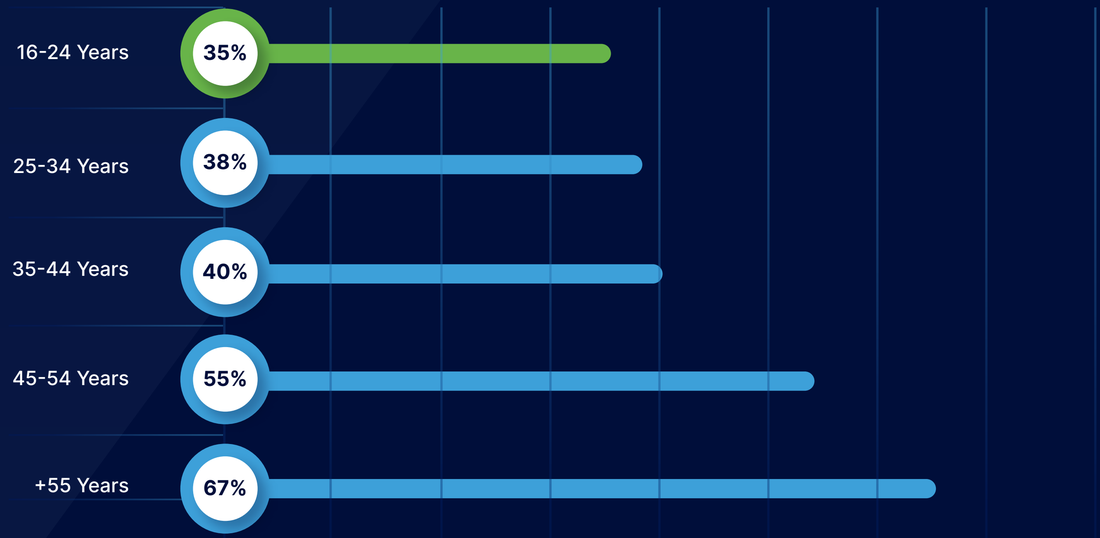
More women than men report being unfamiliar with deepfakes.

63%
Female

41%
Male

Age differences in deepfake awareness

35% of consumers 16 - 24 years of age don't know what deepfakes are



Overall, this highlights a need for increased education and awareness efforts around deepfakes, especially for women and older age groups. As they become more sophisticated and prevalent, it's important for individuals and businesses alike to understand the potential risks associated with them and how to identify them.

The Emotional Impact of Deepfakes

When we analyzed the responses about the experience of being fooled by deepfakes, two categories emerged:

Emotional reactions

Responses such as "Angry," "Felt stupid for not realizing it wasn't true," "Genuinely shocked," "Confusing because it was so realistic," and "Depressed."

Concern of broader threats

Responses such as "Children in need and asking for donations but later found out it's fake," "Criminals could use a victim's identity and use deepfake video to open bank account."

4 Tips for Banks to Prepare for ChatGPT and Deepfake-Enabled Fraud and Financial Crime

Increase public awareness and understanding of deepfakes

Develop educational campaigns targeting lower-aware demographics, such as women and those aged 55 and over. Collaboration with government bodies, media organizations, and technology companies can also help raise awareness of the risks associated with deepfakes and AI-generated text.

Enhance detection and monitoring capabilities

Invest in advanced deepfake detection technologies, tools, and machine learning algorithms. Collaborating with other financial institutions, researchers, and the sharing of information can improve detection methods. Fraud and AML teams need to be trained on the latest deepfake trends, techniques, and detection tools.

Foster a culture of security and vigilance

Educate customers to be cautious when engaging with digital content and report suspicious or potentially fraudulent media. Integrate ChatGPT and deepfake risks into existing security and fraud prevention strategies. Offer guidelines and best practices to customers so that they can verify the authenticity of any communication from the bank.

Advocate for strong regulatory frameworks

Address the risks posed by AI-generated text and deepfakes in the financial sector. Work with regulators to develop policies and encourage the establishment of cross-border collaboration to tackle global deepfake-generated fraud and financial crime.

Conclusion

Trust is the foundation of any long-lasting relationship. The connections between financial institutions and their customers are no exception. Fraud, scams, and other financial crimes undermine that trust and compromise the relationships between both parties.

These exclusive insights into the views of 4,000 UK and US consumers illustrate the impact of fraud and financial crime on consumers. We've revealed that consumers don't differentiate between APP scams and ATO fraud. In either case, they expect their bank to reimburse them. Banks should consider these findings an opportunity to educate customers on protecting themselves from scams and recognize financial crimes like human trafficking and money mule activity.

Banks can improve customer loyalty by minimizing delays in legitimate transactions. Modern customers expect to transact without delays. Indiscriminate interruptions in the customer journey threaten customers' attitudes toward their banks and could even result in churn.

The survey also highlighted the role of social media and other online platforms in enabling various financial crimes, including romance scams, account takeover attacks, and human trafficking. Banks should proactively collaborate with social media companies to protect their customers and promote online safety.

Partnerships will be critical in helping banks prepare for the emerging role of Generative AI technology in financial crime in the coming years – especially with a significant share of respondents unaware of these threats. Deepfake videos, phishing emails created by ChatGPT, and other emerging technologies promise new challenges for banks and financial institutions. That's why banks should immediately educate customers about this technology and work with regulators to develop frameworks to address emerging risks.

While emerging technologies bring significant challenges for banks, AI also brings substantial opportunities to solidify customer loyalty. Most survey respondents, especially younger customers, were likelier to believe AI would protect them from fraud. However, many customers are still uncertain about AI's effectiveness in fraud prevention. As fraudsters get more innovative and aggressive, banks will need to rely more on AI to keep their customers safe. Banks must use this opportunity to educate customers on how AI will keep them safe while delivering the digital banking journeys they have come to expect.

Putting AI at the forefront of your fraud prevention efforts will satisfy your customers and build long-term loyalty as new fraud challenges arise. As a leader in developing safer payment journeys, Feedzai can help secure a loyal customer base and protect financial operations from fraud and financial crime threats.

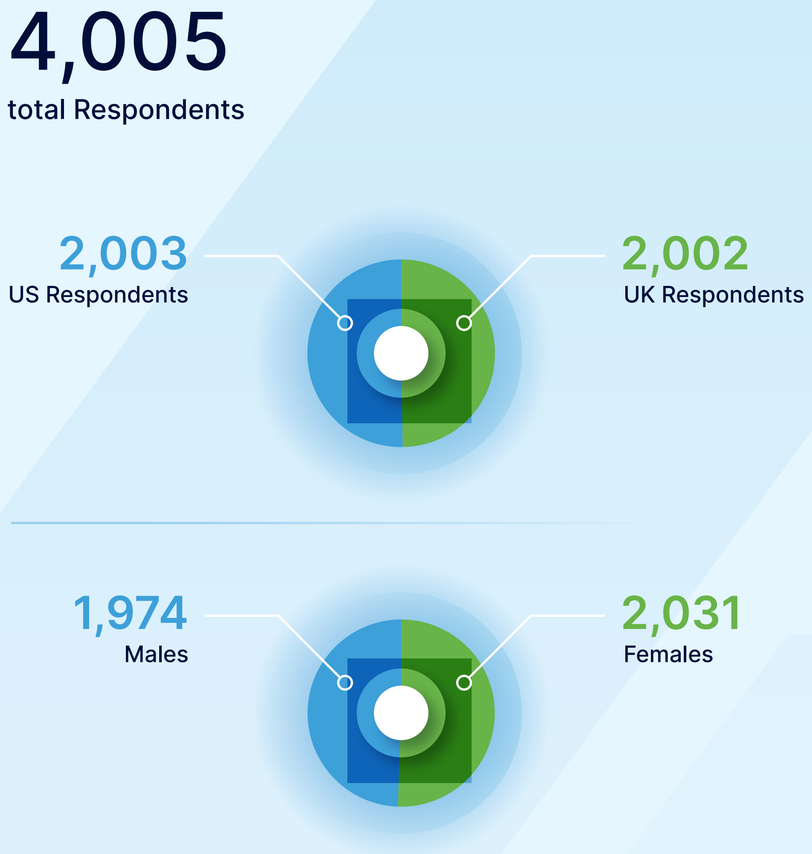
Methodology

To gather insights into the prevalence of financial scams and attitudes toward fraud prevention and protection, we conducted an online survey in partnership with Censuswide, a leading market research company. The survey was conducted using an online access panel, with respondents sourced from Censuswide's panel of participants.

A total of 4,005 respondents participated in the survey, with 2,002 respondents from the UK and 2,003 respondents from the US. Of these respondents, 2,031 were female, and 1,974 were male.

To ensure the integrity of the survey data, all participants were subject to IP-checks and cookie checks. These measures helped to ensure that each respondent could only participate in the survey once, and that the data collected was accurate and reliable.

Overall, the online survey conducted with Censuswide provided valuable insights into the prevalence of financial scams and attitudes towards fraud prevention and protection among a diverse sample of respondents from the UK and US.



feedzai

Transact in Trust.

End-to-end protection from fraud and financial crime.

Feedzai is the world's first RiskOps platform, protecting people and payments with a comprehensive suite of AI-based solutions designed to stop fraud and financial crime. The world's largest financial organizations trust Feedzai to safeguard trillions of dollars of transactions and manage risk while improving the customer experience.

At Feedzai, we understand that trust is essential when it comes to banking, and we undertook this study to evidence our thinking and inform others involved in tackling this challenge.

To ensure your customers feel protected and valued, it's crucial to take a proactive approach to fraud and scam prevention. Technology is there to help but there are a number of aspects to consider. So why not find out where you stand with our no-obligation maturity assessment today?

Our team of experts will help you identify gaps in your fraud and scam prevention strategy and provide recommendations on how to strengthen it. By taking action now, you can build trust with your customers, increase loyalty, and protect your business and customers from fraud and scams. Don't wait - take the first step towards a safer, more secure future today.

Transaction Fraud | Digital Trust | Anti-Money Laundering Suite

Request a Demo

feedzai.com | info@feedzai.com