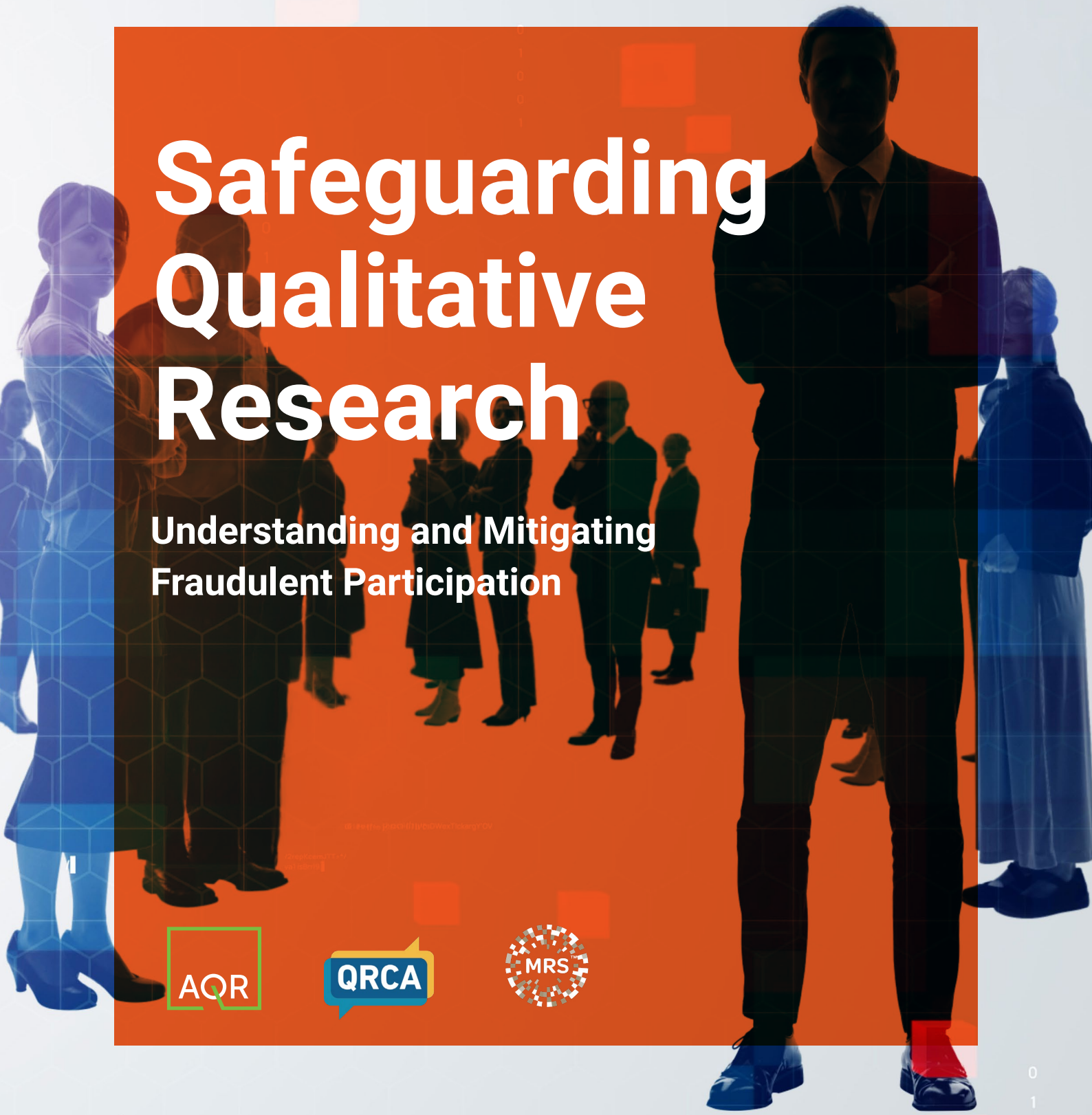
GDQ
GLOBAL DATA QUALITY

Safeguarding Qualitative Research

Understanding and Mitigating Fraudulent Participation



AQR QRCA MRS

Contents

Approach

A working group under the auspices of the Global Data Quality Initiative met roughly monthly over a 6-month period discussing general fraudulent behaviour seen in qualitative research and experiences of AI used to further fraud in qualitative research. In addition to the monthly meetings of the working group, a survey was set up, and sent out via the MRS' newsletter, to gather views on qualitative data quality challenges.

Definitions

Please see globaldataquality.org/Glossary

Fraudulent participation in qualitative research can fall into 4 distinct categories:

Fraudulent participants

Professional participants

Problematic or Enthusiastic participants

Fraudulent participation

Fraudulent participants are defined as:

"Participants who deliberately misrepresent their identity, profiling information, or responses, including organizations that use bots to impersonate participants."

This includes:

- Not responding to questions honestly*
- Using a false name and /or other fabricated personal information
  - Using false ID to impersonate or create a profile
- Taking surveys/participating in research they are not qualified for
- Falsely posing as belonging to a particular demographic group such as age, occupation, etc.
- Overclaiming at the screener*
- Using automation to generate closed-ended and open-ended survey responses

'FRAUDULENT PARTICIPANTS SEEM TO HAVE A HIGHER LEVEL OF FAMILIARITY WITH THE RESEARCH PROCESS THAN GENERAL MEMBERS OF THE PUBLIC WHO PARTICIPATE LESS FREQUENTLY.'

*While not responding to questions honestly and overclaiming can be a clear sign of a fraudulent participant, it is important to consider that sometimes how a screener is constructed and how questions or potential answer choices are presented can force participants into inputting inaccurate answers in lieu of options that fit their situation.

Overclaiming can also be a very natural behaviour given that human beings vary at their ability to accurately recall behaviour, and, therefore, researchers are advised to distinguish between participants who claims that they have used a certain brand three months ago when the actual use occurred six months ago, versus other participants who claims to have used every single brand in a brand list. Acquiescence bias (agreement bias) also happens when participants tend to disproportionately select a positive response.

Fraudulent participants seem to have a higher level of familiarity with the research process than general members of the public who participate less frequently. It is not unreasonable to surmise that fraudulent participants may have started off as professional participants before being flagged due to the large number of studies they have been involved in. However, other routes to become a fraudulent participant are described in guides published online, as well as videos on YouTube and TikTok. These detail how to earn money from research by answering screening surveys dishonestly, adopting fraudulent personas, and working in groups to provide tip offs to new projects.

Responses to a question in a 2023 survey asking participants to define what participant fraud is suggested:

“People lying about their profession so they can participate in studies that they shouldn’t actually qualify for.”

“A participant pretends to be someone who they are not.”

“Answering screening questions untruthfully to participate in surveys (usually paid). Taking part in studies multiple times.”

“Misrepresented qualifications and/or lack of actual knowledge on the subject matter.”

'THESE PEOPLE OFTEN REGISTER ON MULTIPLE FIELDWORK/RECRUITMENT AGENCY PANELS TO INCREASE THEIR CHANCES OF PARTICIPATION.'

Professional participants are defined as:

"Participants who use their participation in qualitative research as a means of income."

Typically, these participants can sometimes fall under the category of 'groupie' or over-researched individuals. Because they apply for a large number of studies, they are more likely to be selected for and participate in research more often and are at high risk of moving into the category of fraudulent participants. These individuals do not answer questions about past participation honestly but—unlike fraudulent participants—may answer the rest of the screening survey honestly or may rely on recruiters that do not ask question on past participation or fail to keep records of how often people participate in their qualitative research studies. There are numerous YouTube and TikTok videos as well as blog posts outlining methods to bypass screener questions.

These people often register to multiple fieldwork/recruitment agency panels to increase their chances of participation. This adds further complexity in detecting those who participate in a large number of studies across agencies.

Problematic participants / enthusiastic participants are defined as:

"Participants who enjoy taking part in research and apply to participate in multiple projects are sometimes known as 'groupies.'".

There is nothing inherently fraudulent about this if their responses are honest; however, there is a risk that information provided by these participants will become poorer in quality due to fatigue and over-familiarity with the language used in research. Their desire to attend more studies may move into a professional or fraudulent participant space.

Fraudulent participation is defined as:

"Providing fraudulent responses to research, possibly by using tools such as ChatGPT or other AI software and/ or presenting responses other than the participants own honest responses."

Which methodologies are at risk of fraudulent Behaviour?

Offline and online (asymmetric) approaches that are completely automated without verification of identity are most at risk for fraudulent behaviour by panelists. This includes, but is not limited to, impersonating a professional, lying about their location, or, at worst, not being a person at all and instead are an automated bot. In such scenarios, the lack of robust identity verification mechanisms makes it easier for fraudulent actors to infiltrate the group, posing significant risks to the integrity of the research data. These methodologies may also suffer from issues such as multiple submissions by the same individual under different aliases, further compromising the validity of the research outcomes.

Online communities that take place over several days will allow some participants to complete the research at unusual times of day, and without live moderation. This means that participants can complete tasks and respond to questions using fraudulent participation methods such as AI responses and without needing to respond in real time.

Online groups or in-depth interviews (IDI) (symmetric and moderated) are the next riskiest for fraudulent participation. Although moderated groups can effectively avoid automated bots and fake participants, panelists do still impersonate someone and/or lie about their qualifications, such as their profession, age, or location. Despite the presence of moderators, these groups face challenges such as the difficulty in verifying the claimed identities and authenticity of participants. The virtual nature of online groups also presents opportunities for participants to use deceptive practices, such as using pre-written responses or sharing answers amongst themselves, which can distort the research findings.

Enhanced measures, such as multi-factor authentication and real-time identity verification, are necessary to mitigate these risks and ensure the credibility of the qualitative research conducted in these environments.

Which target groups are at most risk of being represented by 'bad actor?

Bad actors can make it onto any project of any size and incentive level. The working group identified, anecdotally, that these are most noticeable in business-to-business, luxury goods, automotive, and high net worth studies. However, through review of a payment platform, bad actors were noted as targeting studies of varying incentive levels, size, and topic.

In a one-week snapshot, a UK qualitative recruitment company found that fraudulent participants had applied to studies relating to:

- Student course choices (post-graduate education)
- Social research relating to pay and working conditions
- Vision loss on behalf of a charity
- Medical treatment
- B2B security professionals
- Tradesperson research

There is a perception that projects with a higher incentive are targeted more by bad actors, but these bad actors will apply to most any type of, and to multiple projects. Their gaming of screening surveys could possibly mean that they appear 'on spec' for harder-to-reach audiences where there are naturally fewer other target participants, hence appearing more prevalent. It is also highly possible that typically one-to-one, B2B, and/or higher value projects are where bad actors are more easily identified.

There is also the potential for participants to be thought of as 'bad actors when, in fact, the screening survey used to identify relevant participants has not allowed the most accurate of responses (leading questions, options that do cover the appropriate circumstance) or participants have naturally overclaimed with their responses.

Any target group can eventually be represented by 'bad actors'– fraudulent participants are highly reactive, and they will therefore adapt to the qualifications of the desired target. The lower the incidence (and thus higher the demand) can lead to more

'THE USE OF SOCIAL MEDIA FOR RECRUITING PARTICIPANTS MAKES IT EASIER FOR FRAUDULENT ACTORS TO TARGET THOSE PROJECTS. BUT IT IS ALSO AN ESSENTIAL TOOL FOR RECRUITING.'

fraudulent participants. Today, the typical profiles most often impersonated are likely to be:

- Younger participants (males and females)
- Middle-aged males
- High-income targets
- B2B audiences and other niche audiences.

The use of social media for recruiting participants makes it easier for fraudulent actors to target those projects. But it is also an essential tool for recruiting.

Fraudulent actors look to optimise their efforts by accessing a high number of projects and, in the case of the B2B studies, optimising the individual rewards as well. And they know where to look for projects where they can sign up as participants.

We also see a marked preference for specific markets or cultures (e.g., US or UK participants), because these are typically markets with high volumes of studies and strong currencies and who offer larger incentives. Again, bad actors are focused on efficiency: why create fake accounts in a market where the demand for participants and the pay is relatively low?

How can AI be used by fraudulent participants? How are Fraudulent Participants presenting themselves?

AI presents an opportunity for researchers to use tools to create synthetic participants, enabling faster, cheaper research to gain a deeper understanding of certain target audiences through interrogation of aggregated data and to speed up tasks in the analysis process. AI is based on an online body of knowledge, whereas good quality research sees researchers interrogating real people, whose views evolve faster, and may not be represented in the online body of knowledge. For projects where the client is looking to talk to 'real' people, steps must be taken to ensure that the people participating in the research are indeed genuine.

We must also consider that AI tools can be used by participants to provide 'synthetic' responses to qualitative research. The main methodologies at risk are online, off camera for example:

- Online communities /boards
- Pre-tasks
- Text based chat groups
- Diary tasks

Other examples include participants appearing in online 'on-camera' groups, with their camera switched off, and utilising generative language models to answer questions.

A savvy user of generative AI can use it for fraud in research in different ways:

1. Generative AI can help create convincing/coherent profile data. AI models can help create personas and answer profiling questions by providing likely answers for this persona. For example, if a bad actor wants to claim a high income, using a tool like ChatGPT can help them identify zip/postal codes that would make that claim more realistic; it may even allow a user to answer statement batteries following realistic patterns.

2. However, today, the most useful/common functionality of generative AI, from a bad actor's perspective, is likely the ability to generate a broad range of unique, good quality open-ended responses very quickly (and even translate them on the spot if needed). A single prompt can generate almost unlimited numbers of differentiated, broadly on-topic open-ends, without having to worry about grammar, or even typos.

With the emergence of "Qualitative at Scale" and related methodologies, new data quality challenges arise. Research conducted at scale can introduce additional risks, including compressed delivery time frames for larger samples, a heightened likelihood of non-human participants, and other risks more commonly associated with quantitative research.

Which parts of the research supply chain have a role to play in reducing fraud risk? What might those roles be?

Reducing fraud risk in market research requires a concerted effort across the entire research supply chain. There has been a tendency for some segments to put the burden on the agencies and recruiters, some feeling that 'this is not my problem, but it is for you to deal with.' However, as fraud continues to grow, there is more and more recognition that everyone needs to contribute to ensure the quality of work. Each part of the supply chain has specific roles and responsibilities to help mitigate fraud:

1. Research Clients:

Clients believe that it is up to the recruiters to ensure that only qualified participants make it into their projects. They believe recruiters can tell when someone should not be there and do not understand how unqualified people make it into a project. But, there is a role for clients to play in reducing fraud:

- Demand transparency
- Set standards
- Audit and verify
- Agree to shorter screening surveys
- Recognise that efforts to combat fraud can add time to a project timeline
- Use online tools that prevent access from outside of the region

Additionally, where research clients have their own internal panel from their customer base, there may be measures that they can take internally to ensure that participants signing up are genuine customers, without too much additional burden for participants. Clear conditions and expectations should be communicated to participants should be considered to make it clear to them that any form of fraudulent participation could result in them being removed from the project and panel without payment.

2. Research Agencies:

Like clients, the research agencies see this as an issue that field companies need to manage, but agencies also have a role to play and can help by writing screeners where the qualifiers are not obvious and by keeping screeners short to give spammers less to work with. They can:

- Implement rigorous screening using advanced technologies and methodologies to screen out fraudulent participants - being mindful of how their fieldwork companies/recruiters work.
  - Video screening is one potential tool; or as a minimum, a verbal screening to confirm answers from the original screener. Video screening must also consider whether bias can be introduced at this stage.

'THE ONUS IS ON THESE COMPANIES TO IDENTIFY AND WEED OUT FRAUDULENT PARTICIPANTS. IT TAKES TIME AND MONEY TO AGGRESSIVELY MONITOR FOR FRAUD, WHICH CLIENTS ARE OFTEN NOT WILLING TO OFFSET OR SHARE IN.'

- Training and education: Continuously train staff and work with fieldwork companies on the latest fraud detection techniques and the importance of data integrity.
- Maintain transparency with clients about data collection methods and any potential issues encountered.
- Use online tools that prevent access from outside of the region
- Revert to face-to-face fieldwork for higher risk projects where F2F is feasible. Utilise in-person checks.

3. Fieldwork Companies & Recruiters:

The onus is on these companies to identify and weed out fraudulent participants. It takes time and money to aggressively monitor for fraud, which clients are often not willing to offset or share in. It can be very helpful to communicate, provide feedback and to work with clients on actions that can help reduce fraudulent participants. Specific actions to employ include:

- Quality control, checking for consistency among answers to screener questions as well as comparing to historical data that may be in their record (if in the panel)
- Real-time monitoring
- Data validation
- The use of technology to monitor IP addresses, fake emails, and phone numbers and more
- Stay abreast of the latest methods being used

4. Viewing Facilities

Provide in person assistance to monitor identity documents and potentially re-screen participants on the day as to what is practicable.

All parts of the research supply chain should maintain continual checks for new and emerging technologies that could be utilized to recognize fraud. For example, in the UK there are certain banking platforms that allow easier transfer of funds between markets and there may be similar operations in other markets to be aware of.

What impact is fraudulent behaviour having on the research sector right now?

The increase in survey fraud is having a substantial economic impact on the industry. While researchers and clients may discard bad data without direct financial loss, the labour costs associated with identifying and removing fraudulent data are significant and often uncompensated within project budgets. **This can pose a serious challenge to economic stability of companies recruiting participants.**

Survey fraud can have an even bigger impact on programmatic sample companies. While the number of removals due to fraud will vary from project to project, the numbers can get large. Removing and replacing fraudulent actors will end up impacting costs charged for projects.

The shift to online data collection, which rapidly accelerated during the pandemic, exacerbated these issues. Many qualitative research projects moved online to comply with public-health guidelines without the knowledge and wherewithal to manage projects online. Everyone learned as methodologies, requirements, and behaviours evolved. These online methods allowed for the continuity of research, but they also created new opportunities for fraudulent behaviours, such as misrepresentation and multiple-project participation. The research on fraud in online qualitative research is relatively recent, reflecting the newness of this phenomenon. Fraudulent activity in online qualitative studies, including in-depth interviews, can be more complex to manage than those in quantitative research.

What does fraud look like now?

For **fieldwork agencies and recruiters**, fraud can manifest in several distinct ways:

- Participants might submit applications under different aliases or variations of their name, using different email addresses they have created to try to bypass screening processes or increase their chances of getting selected.

- Some individuals become “professional” participants whereby they regularly contribute to different agencies and lie about their participation history to qualify for more opportunities. They might lie in their responses based on what they believe will work, undermining the integrity of the recruitment process.

- For agencies operating in a single market only, an additional challenge involves individuals from outside of that country attempting to apply and lie about their location, though tell-tale signs are often their contact number or IP address.

- The rise of AI also poses a new challenge, potentially affecting the authenticity of responses and skewing recruitment data.

What does fraud look like for moderators?

Participants with vague responses

Poor camera/online behaviour

Having the 'wrong' knowledge for the topic, i.e., talking broadly but unable to talk specifically

It is important to note that not all poor participant behaviour should be considered fraudulent; participants' adherence to tasks can wane if they are not engaged or if the task is more involved than what has been previously outlined. The methodology itself can contribute to poor adherence at times, and at other times participants can also be less confident with technology or with transparency for legitimate reasons.

What reasonable steps can be taken to reduce fraudulent participation?

In line with best practice, all research invitations should include the key details of the study enabling, genuine participants to make an informed decision about participation. This should include full disclosure of any incentive terms and conditions related to the study. Across all studies, it should be clearly stated - either in the Terms and Conditions of either individual studies, or as part of panel participation - that any dishonest or fraudulent behaviour will result in removal from the study without payment and removal from the panel.

Terms and Conditions of Involvement are key considerations to ensure a correct understanding of payment. These need to be clearly communicated to participants in advance of scheduling them for a project. For example:

- Receiving account names must match the name of the participant, unless participants are children under legal age.

- That recruiters reserve the right to investigate and potentially withhold incentive payments where it appears that individual participants have provided inaccurate or misleading information, especially when matching account details with another participant. *

Researchers, however, should note that when they seek to remove a participant from a study without payment, clear evidence should be provided. Removal may prove time consuming and a reputational risk as well as impacting project timelines. Therefore, avoiding inclusion of potentially fraudulent participants from the outset should be the prioritised approach.

*If a participants' details have matched with another participant, whether banking details or personally identifiable information, care should be taken to ensure that the locally applicable data protection regulations are upheld in discussing the incident. Do not inadvertently share details of other potentially genuine participants or details of any potentially fraudulent participants.

What tools can help?

Many measures can be undertaken to identify and remove fraudulent, professional, and poor-quality participants.

The www.globaldataquality.org/approaches (which is for MRS members only) provides a comprehensive overview of potential measures. Many companies offer anti-fraud software, and survey hosting platforms also provide measures.

A December 2024 article offers suggestions on how to screen out fraudulent participants Understanding and Preventing Participant Fraud in Qualitative Research - QRCA that encapsulates the steps that can be taken in screener construction.

Screener Checks

Actions that can be deployed in surveys to identify and remove bad actors or poor-quality participants early on, include:

- Integrating quality-control questions into the questionnaire
  - Attention checks: Identify participants who are not reading correctly or giving care to the answers chosen.
  - Knowledge checkers: Identify participants who are falsely claiming to have expertise in specific areas.
  - Open-Ended questions: Identify participants who provide poor quality or potentially fake answers.
- Monitoring answering speeds:
  - Monitor the time it takes participants to complete the survey and the time to answer individual questions. Consider removing participants with extreme deviations.
- Unique invitation links for each participant
  - Researchers should prevent multiple attempts from the same invitation link or flag participants associated with duplicate invitation links.
- Identity and location questions
  - Whether the survey is being taken in their first, second or other language may act as an indicator for whether the comprehension of each question by the participant is likely to be high or could vary. This in turn should act as a flag during subsequent screenings (if using a multi-layered screening approach prior to acceptance on the study) to double check understanding. To avoid bias here, additional bias training should be provided to those undertaking screening.

'IN DELETION/ACCESS REQUESTS, DATA PROTECTION TEAMS ARE ADVISED TO COMPLETE DUE DILIGENCE TO VERIFY IDENTITY BEFORE PROVIDING ACCESS.'

- Where the participant is completing the screening survey, ask whether they are in the target country/region. This question is likely to be completed fraudulently by fraudulent participants; however, if subsequently it is realised that the participant is outside of the desired country/region, the researcher may be able to rely on Terms and Conditions of participation to remove them from the session.

- Use knowledge-based questions within the screener relating to the area being recruited from. These could be hyper-local but may still be able to be faked.

Database Usage and Tagging

Where it is legally permissible to tag participants, do so carefully to indicate that they are/have:

- Known fraudulent or professional participants*

- Have failed one or more quality checks previously*

- Considered high risk by the research for other reasons.*

However, in opt-in databases, fraudulent/professional participants who are removed from mailing lists can often unsubscribe/delete accounts* and then resubscribe or simply create a new alias.

*Under GDPR in Europe, the UK, and countries with equivalency status, individuals will usually have the right to access their data, and the right to be deleted. These should be upheld in all circumstances. Therefore, researchers are advised to make appropriate notes with only factual language. In deletion/access requests, data protection teams are advised to complete due diligence to verify identity before providing access. This should be in line with the information provided on signup. In cases where the account is fraudulent or is one of multiple created by a fraudulent individual, the participant may not be able to provide information that is consistent with that provided on signup.

'WHILE A DETERMINED FRAUDSTER CAN EASILY OBTAIN A FAKE ID, EXTRA STEPS CAN BE TAKEN TO MITIGATE THIS RISK'

Review Participant Survey Taking History

Assess the participants to identify behaviours and signals that could identify them as bad actors:

- Risk Scoring
  Check for previous fraudulent activity associated with the participant and their IP address to assess the risk inherit in participants' responses. Use of other factors can contribute to this information and be used to generate a risk score. AI can also be used to build models that predict riskiness based on a larger pool of participants.

- IP Checks
  Check for fraudulent activity associated with the IP address and use it to validate their location. Consider blocking VPNs and Proxies, as these are often used to mask a fraudster's actual location.

- Previous Participation
  Assess the frequency of participation in previous interviews and look for red flags that can be a precursor to a bad actor. This can include someone who is always late so they cannot be rechecked and/or someone who (if online) is hard to hear in the hopes they will be paid and sent. These factors may be added to the risk score. It can also help to set a threshold that limits the number of sessions participants can attend over a given period.

Personal Identity Verification

Require a participant to provide a copy of a government-issued ID or license (medical or any industry that licenses their members) to prove identity. While a determined fraudster can easily obtain a fake ID, extra steps can be taken to mitigate this risk:

- Validate the ID with a third-party service

- Ask participants to pose for and send a selfie with their ID

- Ask participants to pose for a selfie with their ID and an object such as:
  - The product being researched
  - An everyday object that most panelists would have, like a pen
  - A piece of paper with their name and a handwritten code unique to their session
  - A LinkedIn search, while not foolproof, can also be a way to verify identities.

Viewing facilities can act as a valuable assistant during face-to-face fieldwork in a way that hotels without hosts or virtual options cannot. Discuss what support viewing facilities or a local host can provide in checking participant identity documents and ensure that data protection instructions, such as a statement of work, allow for this. Where companies are unable to share full details of

'SOME CHECKS AND RULES CAN BE ENFORCED WITHIN THE STUDY; IF PARTICIPANTS DO NOT COMPLY OR FAIL, THEN THE SESSION CAN BE ENDED'

participants with viewing facilities or hosts, the moderator should consider whether they are the best placed person to check IDs.

In-Field Validation and Screening

A researcher may be faced with starting a session and still have concerns about fraudulent participation. Some checks and rules can be enforced within the study; if participants do not comply or fail, then the session can be ended:

- Require webcams to be turned on and participants to be visible
    - Require VPNs and Proxies to be turned off
    - Do not accept Google Voice
    - Ask the participants questions to validate their identity and location while cross-referencing with the information available to you
    - For example, ask where they live or work. Then, see if this matches their survey answers and IP location. You could take this further by asking them how the weather has been in their city and checking weather reports. You could also ask where their office is located and check their company site to verify this.
    - As part of the confirmation email/ process include a disclaimer that states that if there is doubt on the identity or truthfulness of answers provided, the session will be ended, and the participant is at risk of losing the incentive.
- Suspicious images could be verified with reverse image search tools that check for identical images elsewhere online, such as Google Images, Bing Image Search, and Yahoo Image Search. Some third-party solutions provide biometric verification services, including AI facial recognition, which could further deter fraudsters.
- Responses can be checked using an AI checker; this needs to be done on an ad-hoc basis due to the time involved.
- Consider re-screening prior to the start of the session. This may mean communicating to all parties involved that re-screening will happen and anybody failing rescreens will be asked to leave without payment.

Specifically, how to prevent disruption to research quality from the use of AI by participants?

The world is learning to work with AI and its rapid evolution, and researchers are assessing how to best use it for our needs in the most appropriate ways. Governments are looking to understand how and if AI usage should be regulated, with the EU laying out the world's first law around AI. Similarly, the market research industry is still in the early stages of understanding how to identify and prevent fraudulent AI usage.

AI is another tool in a fraudulent participant's belt. This means there is still a fraudulent individual pulling the strings, and the measures referred to earlier in this document can still help identify fraudulent participants using AI for their purposes.

Fight AI with AI

AI predictive risk scoring could be used to assess the likelihood of a participant being fraudulent based on their activity and of previous participants. It could also be used to identify participants using generative AI to create unique profiles.

Human Validation

Validate that an actual human being is behind the answers.

- CAPTCHA technology to identify any unsophisticated automation attempts
- Telephone validation and verification of IDs at the recruitment stage
- Requiring participants to record a video or audio response as part of a survey
- Require participants to keep their webcam on and remain visible during sessions to prevent them from using AI to generate responses

Monitor for Exiting Behaviours

Identify participants who display behaviours that could indicate they are leaving the survey to get answers from an AI solution, such as:

- Using the copy and/or paste function on their browsers
- Attempting to leave their current browser tab
- Set time limits for participants to answer questions

Lastly, as AI becomes increasingly incorporated into daily life, genuine panelists may simply need a reminder that we are after their opinions based on their experiences, and they should not use AI to formulate an opinion and to help create their answers. In research we need their authentic selves.

What is the risk of using measures to reduce fraudulent participation? What is too much?

Researchers should consider numerous risks, including legal risks, participant attrition, and excessive removals (removing participants from projects too frequently). They should ensure that the measures they are using are appropriate and use a blend of solutions - it may not be economically viable to run every possible check on all participants. There also needs to be a balance between risk mitigation and maintaining positive participant experience.

Legal Risks

When using measures to combat fraudulent participants, researchers should consider which practices best suit their research and ensure consent is collected where applicable. AI could be fought with AI, but unlike fraudulent participants, researchers must be extra cautious in their usage of AI, ensure they are legally compliant and are mindful of how the data is utilised. Many verification measures involve handling sensitive PII, so ensure data is handled in compliance with the appropriate laws and regulations, such as GDPR.

Note that laws and regulations vary in countries outside of Europe and from state to state within the U.S.

Mitigation: Consult with in-house or external experts on privacy laws. Ensure that any external solutions handle data appropriately on their side.

Participant Attrition

Genuine participants could be frustrated or deterred by the checks and balances they are subject to:

- Intrusive measures such as biometric and facial verification
  - Mitigation: If possible, only run this check once and implement a “trusted-participant status” to identify vetted and genuine participants. Inform panelists of the reason for this check and the status they will receive when completing the verification.
- Repetitive checks like attention checkers and open ends
  - Mitigation: Limit this type of check to one or two questions per participant. If participants have a trusted-participant status, consider if these are needed. Change the questions used over time to avoid participants becoming overfamiliar.

- Wasting time after answering many questions and then being rejected from an opportunity to participate
  - Mitigation: Screen participants as early as possible, be courteous, and thank them when rejecting them as a participant

Excessive Removals

More checks mean a greater chance of catching bad actors. However, it also generates more hurdles for genuine participants who may fail checks.

Mitigation: Grade security measures by severity and consider removing participants or flagging based on failing either the most severe or a combination of measures.

Summary

As fraud continues to grow, it will take all parts of the research supply chain to continually work together to protect data integrity within qualitative research. This will mean continual assessment of tools, the landscape of fraud, and measures that are available and positively contribute to the experience for genuine participants.

GDQ

GLOBAL DATA QUALITY