PARTICIPANT INTEGRITY INITIATIVE

June 2022

KNow Research

In the Summer of 2022, the team at KNow Research embarked on an internal project to better understand the widespread issue of research participant fraud in the insights industry. We looked into the matter to understand the issue at large and ways we can work with our partners to prevent it as much as possible from impacting the quality of our studies.

Our goal: refine our internal practices and provide thought starters and resources to the insights industry as a whole to protect the integrity of qualitative insights.

Picture It:

You recruit 12 participants for one-one-one interviews from a quantitative study that targeted US-based, C-Suite professionals. You do your due diligence to invite those who gave thoughtful and relevant responses in the initial quant survey. You schedule follow-up interviews, and to your initial delight, you hit the nail on the head with some outstanding professionals who were exactly who you hoped had taken your survey!

Until you meet 'George Henry'. 'George' claimed to be a CEO for an NYC based tech company. The time arrives, you're on the line, and 'George' enters, though doesn't turn his camera on. You greet 'George' and ask that he kindly turns on his webcam. He claims to struggle to figure out how to do this and asks if it's necessary. You remind him that this was criteria laid out in the study and that he tries again. At last, his camera turns on, and you see a shadowy figure in a dim room. You ask if he can turn a light on or move into a brighter area, to which he replies that he doesn't have a brighter room.

You begin the conversation with a typical warmup – *what do you do for work and for fun?* To which 'George' replies a cryptic answer that's difficult to understand. You proceed with some questions to confirm his role in topic of the research, to which his answers cryptically – '*yes, I decide on that, and think are important to employees'.* He is soft spoken and with a thick accent and you worry – this does not appear to be a CEO of a tech company in NYC, but how can you know for sure? After a couple minutes of choppy elusive conversation, you make the call that 'George' is not in fact the person he is claiming to be and dismiss him, though without any concrete evidence. You feel uncomfortable and awkward in doing so – what do you say? You decide to use the excuse of a bad connection and that you can't hear him well enough to proceed, thank him for his time and end the call. You later confirm by running his IP address that George was actually located outside the US. Your suspicions were confirmed – he was not who you thought he was nor needed for your study. You're now down one interview, don't know how to explain the situation to your stakeholders, are concerned about the quality of the overall sample and don't know how to prevent this from happening again on this study – or any other for that matter.

How did this happen?

Your initial quantitative study was thoughtfully designed to 'weed out' anyone who did not in fact appear to be a C-Suite professional, including 'trick' questions to ensure participants were

paying attention and numerous open-end questions that asked detailed questions about their decision-making criteria. Your quantitative partner employed protocols to scrub the data for irrelevant or suspect responses using algorithms and parameters set to detect survey fraud. Your team manually scanned open end responses to check for sensical answers that gave confidence in the 400 completes. So how did this one slip into the qualitative round? And even more concerning – **if this was just 1 out of your 12 qualitative interviews, how many more potentially issued existed in the quant data that you just reported on?**

This is a true story, one of unfortunately many incidents that we've experienced over the last year in our projects at KNow. It started becoming sadly predictable that at least one fraudulent participant would infiltrate our studies, regardless of which recruitment method was used. This inspired us to do our own investigatory research into the issue at large to figure out how we could prevent this from happening.

Why it matters for both quant AND qual

Insights professionals strive to construct thoughtful strategic research design that ensures we ask the right questions in the right way to get the right answers. Research participants are thoroughly screened and vetted to be sure they are qualified for the study, but yet, there are still many ways that component of studies can be compromised.

It's our goal as a company to ensure that participants we speak with can deliver the quality information our clients expect.

However, in the insights industry as a whole, we see more emphasis on online sample fraud and its impact on quantitative studies. While the quantity and origin of much of the fraud stems from these sources, other recruitment methods are also susceptible and impact the qualitative research we do.

And our stakeholders and clients want and expect it as well. As one of our client partners says: ***"Qualitative work necessarily places even greater emphasis on the quality of participants than quantitative work due to the cost and time dedicated to each respondent. Participant quality is paramount to delivering valuable insights, but we haven't seen the same emphasis on fraud prevention and participant quality in the world of qualitative recruitment as we've seen in quantitative panel management. We place a premium on any partner agencies that recognize how vital it is to guarantee that our budgets are well spent on quality respondents." –***
Customer Intelligence Associate Director, Online Audio and Video Media Company

How we see it impacting study quality

Alarmingly, in the past 12 months, we've experienced fraud stemming from all following qualitative recruitment methods:

- **Quantitative survey panels:** when recruiting qualitative participants from a sample who just completed a related quantitative study
- **Traditional qualitative recruiters:** when recruiting by pre-screen survey and phone
- **Direct from widgets/banners on websites:** when sourcing participants based on who's engaged with a brand/company
- **DIY qualitative recruiting tools:** when using self-service recruiting tools
- **Social media:** when sourcing participants from the general public by posting an invitation on a social channel
- **Email lists:** when sending an invitation to a vetted list

No matter where it comes from, incidents of fraud are much more up-close and personal in qualitative research than as a line item in a quantitative excel file.

What we learned

The Big Picture: Industry Learnings

Research fraud is rampant, and on the rise

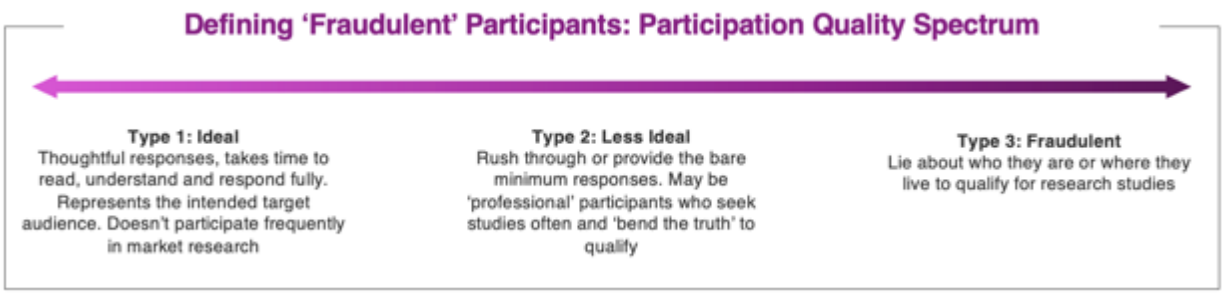
There's no shortage of discussion around the issue of fraud in market research. The pandemic moved more qualitative online and moved more people to look for opportunities to make additional/supplemental income through participating in studies and given more remote access to those studies globally.

- Research providers may routinely remove **20-30%** of their sample due to fraud (some up to 90%)
- Professional survey takers have been found to take **upwards of 20 surveys a day**
- In an IA webinar poll*, **51% of research providers had experienced fraud in the last week alone**, and **73% in the last 3 months**
- **B2B studies and hard-to-reach samples can see more fraud** due to higher incentives; higher incentives = more attractive studies = higher fraud
- **There is no industry standard for what constitutes 'fraudulent'**, leading to different standards across software and 'best practices'

The Participant Perspective

We decided to go straight to the source – to the 'fraudsters' and 'professional participants' themselves, to understand their motivations and strategies for qualifying for studies so we could determine how to better safeguard against them.

To do this, we conducted a 2-fold approach, first with professional participants' (**Type 2: Less Ideal**), and then with 'fraudulent participants' (**Type 3: Fraudulent**)



Type 2: Less Ideal: We held an in-person focus group to learn from this group.

They participate in research frequently and were open and eloquent, offering extensive detailed explanations in their responses and were quite transparent – everything a qualitative researcher could ask for.

However, they violate industry recruitment best practices. In participant screeners, we build in questions in attempt to 'weed out' people who have taken research studies recently (particularly on the topic of interest), in addition to the standard demographic questions that tend to filter out those who fall above or below a certain age threshold.

This group has often figured out their way around these questions, **and often bend the truth to make their way into studies**. Here are some staggering facts we learned about their world of a professional participant:

- They **proactively** scan the web for studies in places like social media, Craigslist, and Reddit
- Research studies for them often surmount to a full-time job with month income upwards of **$3-5K**
- **Age** is the most common place participants may lie to participate – they know what the cutoffs tend to be
- Some told us that **they were encouraged to stretch the truth** in a screener to qualify for a study

"With this movie company, you have to watch the movie with a child and so I had my girlfriend come and sit there. She's 32, but she looks like she's young." *– Jasen*

"I can fake my opinion. Tomorrow, I'm Democrat. Today, Republican." *– Julius*

"Just the other day somebody coached me about a study. I'm not married. I don't have kids. But now, I have a kid!" *– Erhan*

Type 3: Fraudulent: We conducted webcam interviews to learn from this group.

We carefully recruited participants whom we had previously identified as fraudulent – the ones we had to awkwardly dismiss from interviews and groups.

We began like we would any other study – sending out an email invite to a list of emails we had collected from past studies with a link for them to book a slot to discuss 'the research experience' with us for a $50 incentive. We opened up a variety of slots to allow participants flexibility to book but did not anticipate what happened next – **within minutes, we had 100+ signups!** The invitation link had been passed around like wildfire. Retrospectively we should have anticipated this – of course the link was passed around to a broad network – we are recruiting fraudulent participants! We cancelled those who were not on our original list saying that it was only open to those on our original database.

We then vetted our participants'' IP address to see if what they said matched their location using IP Quality Score (screening to detect fraudulent web activity by assigning a quality score to each IP address: the higher the score, the more malevolent the online behavior detected). While people may have legitimate reasons to change their online location through VPNs, for instance, this due diligence can help confirm or deny your spidey sense!

Learnings from Fraudulent Participants

Location

- Many told us that they lived in Western US cities like Portland or Dallas or LA, though their IP addresses told us they signed up for the study in EST. When asked about this discrepancy, they all had the same story– that they were visiting others or had traveled to the east coast at the time that they signed up for our study.
- We asked certain questions like 'how's the weather today in Portland'? to which they responded it was a very nice day. When looking up the weather, it was typical Portland – rainy and in the 50's.
- We pressed one who was in front of a curtain: could he open it to let some light in? He refused, saying that he felt uncomfortable doing that since there was another house across the way.

Career status

- As part of the conversation warmup, we asked typical questions like what they do for a living; they all had very detailed specific responses. One participant, 'Jessica', lived in 'Dallas City' and said she was an accounting student at University of Texas. We looked up the school, and low and behold – 'Accounting' is the first major listed on the site. An easy cover story.

Incentives

- We asked what kinds of incentives attract them the most to studies. Most preferred online monetary gift cards that weren't store specific.
- Many were 'ok' with incentives that are mailed to their residence. This surprised us since we knew that they were located outside of the US, which would theoretically make mailing incentives impossible. However, we later discovered that some scammers use a P.O. box and have a locally based person collect incentives to then mail or deposit to their actual address or account outside the US.

Other discrepancies

- Since these participants had all been ousted from previous studies, we had audition videos of one of them – 'Tristan' – and reviewed it prior to interviewing him again. To our surprise, the video featured a young woman, not the 'Tristan', the man we were now speaking with! We asked 'Tristan' why a woman had shown up under his name for the last study, and he claimed to not know, however, admitted that he shares an email address and linked PayPal account with 2 friends for business purposes; they must have given it to someone to participate.
- Perhaps the most climactic participant we interviewed, under the name of 'Mike', was actually the same participant we had interviewed the day before who went by 'Jessica'! She showed up this time with a mask on her face, and upon asking if she was actually Jessica from before, outright denied it and insisted she was 'Mike'. We had to hand it to her for sticking to her story!

In sum – these participants are VERY good at sticking to their stories. They also pass along study opportunities with others through social media and WhatsApp groups, scan social media groups and forums for such opportunities.

Search terms used on Facebook, Instagram, Twitter, WhatsApp, Craigslist & Reddit groups/pages	**Hashtags**
▪ research participants ▪ focusgroup.org ▪ insightspace	▪ #focus group participant ▪ #research participant ▪ #cloudresearch ▪ #researchmethod ▪ #focusgroup ▪ #paidresearch ▪ #researchparticipant

Partner Perspective: Best practices from our community

How we can work together as an industry to prevent fraudulent behavior from impacting studies

We checked in with **our partners** to determine how they have noticed integrity being compromised and to compile a list of proactive and reactive measures employed to ensure quality participants.

We learned about many measures to prevent and mitigate fraud that are constantly improving and becoming more sophisticated, but so do scammers' efforts to work around them.

As one of our partners, Lilah Raynor at Logica Research put it: ***"It is a bit of a game whack-a-mole. Fraudsters figure out how to work around it. We spend a lot of time managing field and data quality on top of this to ensure we don't have fraud and work with our recruiting sample partners to ensure great quality respondents."***

Our partners' actions and recommendations to reduce fraud

We want to prevent our team from the awkward and stressful experience of being in the hot seat and having to make the call whether to dismiss someone for they suspect to be fraudulent. The following is a list of suggested proactive best practices to eliminate fraud before fieldwork

#1 Consider some/all of the following proactive techniques:

- Pre-screen via phone in before admitting them as a panel member or for a specific study. *Be wary of Google voice users who do not pick up the phone and/or red flag them if they give general or vague answers, ask 'which study is this again?', ask immediately about incentives or who don't resonate as the person described in the screener demographically or geographically*
- Include and review open ended responses and 'trick' questions in surveys and screeners
- Lock survey links so they cannot be shared
- Automatically update panel participants' demographic information (e.g., age) vs. letting them update it on their own in a screener to try to get into a study
- Asses if email addresses match the provided names
- Build in video audition questions into screeners and/or ask panelists to provide link to a social media account for dual factor verification
- Use automated tools that screen for habitual survey taking, inattentive responses and scanning for bot farm networks, like 'Research Defender'
- IP screen ('digital fingerprinting') to examine participants past activity e.g., frequent survey taking or other acts of fraud
- Block known IP addresses and VPNs via tools like 'Cloudfare'
- Keep fraudulent participants in a database, as opposed to removing them, to ensure they will not be contacted for a study again and prevent them from signing up again for the panel under a different identity
- Overrecruit (when budget allows)

#2 Ask questions of your partners to ensure you're thinking of all the potential ways to prevent fraud:

Knowing the right questions to ask your partners is key; be sure to include the following questions when kicking off a project and determining your sample source(s). One of our clients recommends carving out time for a 'fraud day' in which everyone on the project sits down to determine all the ways in which fraud could impact the project and what we can put in place to prevent as much of it as possible.

- How do you screen participants?
- What source(s) is the recruit coming from? *Note that social media recruitment has a high likelihood for fraud vs. vetted database.*
- What types of automated and manual checks do you employ to ensure data quality? Do you collect and check recruited participants' IP addresses? Do you re-screen recruits on the phone and/or by video to verify their identity and story?
- Do you have a referral program? What percentage of their past fraudulent participants came from referral links vs direct signup?

When sourcing panel and having these conversions, consider what your partner has in place and what additional measures you may have to take to ensure quality.

#3 Reactive measures; what to do once you're in field

- Go back to your proactive tools if you notice fraud popping up once you're in field:
  - Run respondent IP addresses in a tool like 'Clean Talk' or 'IP Quality Score'
  - Manually review open-end survey responses
  - Use algorithms or automated tools that check for suspect survey patterns, time thresholds, nonsensical, insufficient, or repeat open-ended responses, e.g., Research Defender'
  - Employ a re-captcha interface to validate whether there is a human user or bot based on cursor movements or click patterns
- Re-screen recruited participants in the virtual waiting room before a session begins. *If the participant doesn't turn their webcam on or and seems hesitant to do so, this is often an indication that they may be fraudulent*

- Ask warmup questions that give you confidence that they are who and where they say they are, e.g., weather related questions, specific questions about their work, and where they are located while cross-checking their IP location
- If you *still* aren't confident, you can ask then to show their photo ID to verify their identity (use at your own comfort level and discretion)

Conclusions:

The threat of scammers and fraud in research (or any other industry, for that matter) will never be completely avoided. Instead, proactively expect it and work to prevent as much as possible from happening on your studies. The question should not be 'if' it will happen in a study but 'to what extent'. And the goal should be to make the extent as small as possible.

By calling attention to the integrity gap, our industry can feel more empowered and confident in the current (and developing) mitigating solutions. **While sophisticated automated tools have emerged and will continue to do so, we still encourage using manual checks.** Ensure your project timelines account for fraud prevention steps across to ensure quality participants and data from pre-field, in-field and post-field.

At KNow Research, what started as frustrating and sometimes panic—inducing encounters in our qualitative research has turned into an opportunity to learn and contribute to this important industry-wide endeavor that will ultimately help us do our best work for our clients.

We'd like to thank our partners for contributing to this initiative:

- Logica Research
- Longitudes Group
- Rep Data
- Watch Lab
- Fieldwork
- HubUX
- User Interviews

If you're interested in learning more, you may refer to the following sources:

- New MR: Solving the Participant Crisis
- Happy Market Research Podcast:
  - Characteristics of a Fraudulent Respondent and how to Filter Them Through Survey Design
  - How to Avoid Fraudulent Respondents with Dr. Leib Litman, CEO at CloudResearch
- Insights Association: Online Sample Fraud: Causes, Costs & Cures - Continuing the Conversation, March 25, 2022
- Greenbook: Market Research Fraud: Distributed Survey Farms Exposed
- Science Direct: https://www.sciencedirect.com/science/article/pii/S2214782921000415

Stay Tuned: We're not alone in our concern about qualitative study quality and participant integrity. Industry associations like the Insights Association's Sample and Data Quality Task Force and CASE4Quality are working to illuminate and mitigate fraud in online research, and the sampling landscape. We're getting involved in these work groups to ensure that qualitative studies/situations are included in the dialogue.

At KNow, we are committed to collaboration, and will continue to explore fraud prevention strategies with our partners. What are your participant integrity tips? admin@knowresearch.com