PARTICIPANT INTEGRITY INITIATIVE

In the Summer of 2022, 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 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 existed in the quant data that you just reported on?**

This is a true story, one of unfortunately many incidents that have increased in our industry in recent years. Despite our best efforts, it became sadly predictable that at least one fraudulent participant would infiltrate each study, regardless of which recruitment method we used. This inspired us to do our own investigatory research in the Summer of 2022 to determine how to prevent this from happening. And it's inspired us to continue monitoring our integrity incidences to ensure we're always exploring and innovating ways to prevent as many cases as possible.

Why integrity 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 quality insights. Research participants are thoroughly screened and vetted to be sure they are qualified for the study, 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.

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 fraud impacts study quality

Alarmingly, 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
- **Third party 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 clients' customer list or database

No matter where they come 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

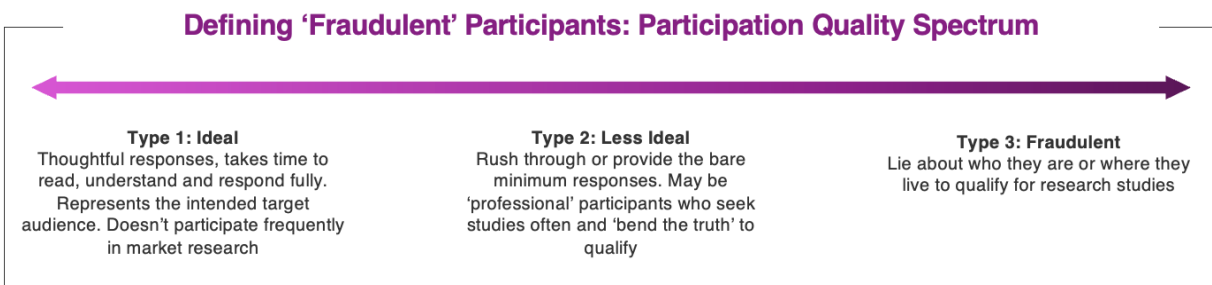### The Big Picture: Industry Learnings
Research fraud is rampant, and on the rise.

There's no shortage of discussion around the issue of fraud in market research. Twos key reasons behind the uptick in qualitative fraud during the pandemic stemmed from 1. qualitative methods moving online (vs. in person) and 2. individuals seeking additional income opportunities through study participation. On the other side of the pandemic we see no slowing down or reversal of the trend, if anything communities like Paid for Your Say have increased visibility of our studies and actively encourage participants to bend the truth to qualify.

The Extent of the Problem
- 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 a 2022 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**; their higher incentives make them more attractive studies and lead to greater likelihood for 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**)

Defining 'Fraudulent' Participants: Participation Quality Spectrum

Type 1: Ideal
Thoughtful responses, takes time to read, understand and respond fully. Represents the intended target audience. Doesn't participate frequently in market research

Type 2: Less Ideal
Rush through or provide the bare minimum responses. May be 'professional' participants who seek studies often and 'bend the truth' to qualify

Type 3: Fraudulent
Lie about who they are or where they live to qualify for research studies

KNow
RESEARCH

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

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

- They **proactively** scan social media, Craigslist, Reddit and other digital sources for study links/information and tips on how to get past screeners

Search terms and hashtags used to mine for studies

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

- Research studies for them often surmount to a full-time job with a monthly 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 in the past.

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.

Exhibit 1: The Signup List

We then vetted our participants' IP addresses 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! We've continued to use this tool as a helpful validation technique when we suspect a fraudulent participant.

Learnings from Fraudulent Participants

Location
- Many said 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', was a student in 'Dallas City.' She said she went to 'The University of Texas.' When asked her major, said she 'accounting'. We Googled 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 an articulation video 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' 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.

Partner Perspective: Best practices from our community
How we can work together as an industry to prevent fraudulent behavior from impacting studies

KNow
RESEARCH

We checked in with **our partners** who support our qualitative studies to determine how they noticed integrity being compromised, and compiled a list of proactive and reactive measures they employ to ensure quality participants.

We learned about many measures to prevent and mitigate fraud that are constantly improving and becoming more sophisticated. However, as our safeguards improve, so to do the scammers' efforts to work around them.

As one of our trusted partners 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.***"

How to Prevent Fraud

To prevent our team from the awkward and stressful experience of being in the hot seat and having to make the call about whether to dismiss someone they suspect of being fraudulent we've compiled a list of suggested proactive best practices to eliminate fraud *before* encountering it during fieldwork:

#1 Consider some/all of the following proactive techniques
- Rescreen participants sourced from client lists, quant panels, or DIY recruiting tools on the phone, ensuring you're able to hear their voice and confirm their participation before fieldwork. Beware 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 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 where the survey platform allows
- Ensure recruitment partners automatically update their panelists' 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
- Require video articulation questions in all screeners to not only ensure participants can speak eloquently and accurately to the study topic, but also that the individual you see aligns with their provided screener responses
- Ask that participants provide a link to a social media account for dual factor verification
- Screen IP addresses to examine participants past activity e.g., frequent survey taking or other acts of fraud
- Keep track of fraudulent participants in a database (e.g. name, email, location, video articulation), 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 (as budget allows)

#2 Talk to partners and clients to ensure you're thinking of all the potential ways to prevent fraud
Knowing the right questions to ask your qualitative partners is key; be sure to include the following questions when kicking off a project and determining your sample source(s):
- How do you screen participants?

KNow
RESEARCH

8

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

Additionally, when brands provide a customer list to recruit from, it is important to understand the following:
- Where does the list come from? (e.g. a pop-up on the website, email opt-in, customer event…)
- How old is the list? How recently did customers opt-in?
- How has the list been vetted? (e.g. customer login verification, proof of customer engagement)

#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
- Re-screen recruited participants in the virtual waiting room *before* the session or group goes live to your clients.
    - o 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
    - o 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, consider asking them to show their photo ID to verify their identity (use at your own comfort level and discretion)
- When you conclude that a participant is likely not who they say, discretely remove them from the session. You may send them a cancellation notice that you were unable to match their name, time zone, email etc. with what was on record for the invitee, so per your company policy, they are unable to participate and will not receive an incentive.

Conclusions

We will always be at risk of the threat of scammers and fraud in research (or any other industry, for that matter). Instead, proactively expect these situations to arise 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'. 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

KNow
RESEARCH

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

Stay Tuned

We're not alone in our concern about qualitative study quality and participant integrity. Industry associations like the Insights Association's Council for Data Integrity 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

We'd like to thank our partners who contributed to this work

- Logica Research
- Longitudes Group
- Rep Data
- Watch Lab
- Fieldwork
- HubUX
- User Interviews
- SyncScript
- Broad Project Solutions
- Lexicon & Line

For some of the latest on the topic, you may refer to the following sources:

- Greenbook, *Online Survey Frauds in Market Research: Challenges and Solutions*
- Insights Association, MRS, SampleCon & ESOMAR Join Forces To Fight Fraud, Boost Data Quality
- Insights Association: Council for Data Integrity
- Kantar: *Is Panel Fraud the new Ad Fraud? The shocking issue affecting market research solved with AI.*
- Nasdaq: *Businesses and Investors are Losing Billions to Fraudulent Market Research Data. Here's How to Fix It*
- Quirks: *Minimizing fraud risk from generative AI in marketing research: A guide*
- Recollective: *Mitigating Fraud in Online Qualitative Research*

KNow
RESEARCH