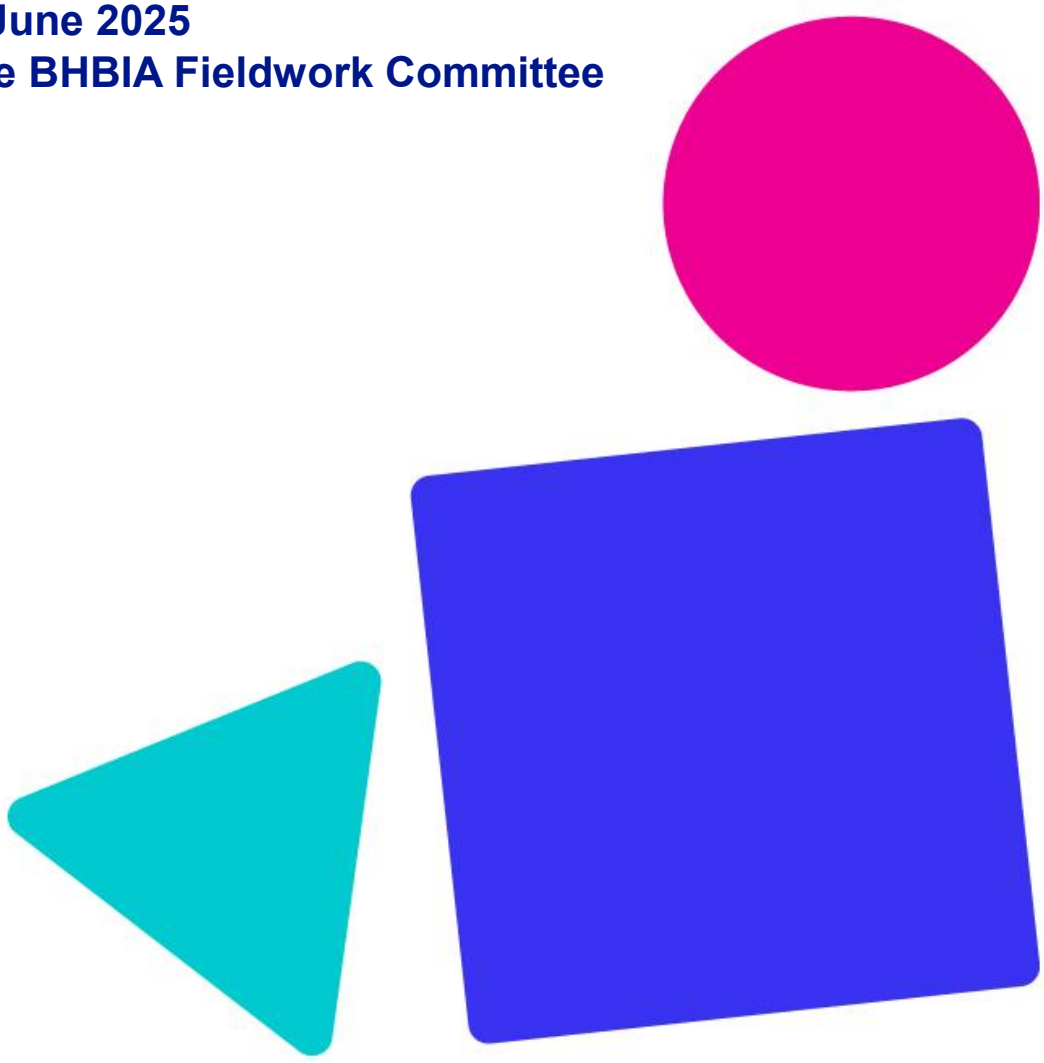
BHBIA

bhbia.org.uk

Preventing Fraudulent Respondents In Primary Market Research

Published 18th June 2025
Produced by the BHBIA Fieldwork Committee



BHBIA

bhbia.org.uk

Preventing Fraudulent Respondents In Primary Market Research

Published 18th June 2025 | Produced by the BHBIA Fieldwork Committee

Contents

Introduction

As the pharmaceutical industry continues to adopt rapid advancements in technology and artificial intelligence, the demand for high-quality, accurate insights from primary market research is growing fast. At the same time, the risk of fraudulent respondents is an increasing concern - with industry data suggesting that **5% of total honoraria or incentive spend** is lost to fraud[1]. While this figure primarily reflects consumer research, where fraud is more prevalent, healthcare market research is not immune. High incentives can attract bad actors, though misrepresentation is more difficult where robust verification processes are in place.

In this context, "fraudulent" refers to participants who misrepresent themselves, provide false information, or attempt to take part in a study more than once - often for personal financial gain. These respondents can infiltrate both qualitative and quantitative research, undermining the quality and reliability of the data.

Given how central market research is to product development, marketing strategies, launch plans, and customer engagement, spotting and stopping respondent fraud is critical. If left unchecked, it can distort insights, lead to poor decision-making, and damage stakeholder relationships.

This guide explores why tackling respondent fraud matters in healthcare market research and outlines practical strategies for identifying and preventing it. By following this guidance, teams can better manage the risk of fraud and ensure the insights they rely on are credible and actionable.

Identifying Fraud in Primary Research

Qualitative Research

While fraud is less common in qualitative research than in quantitative studies, it still happens, especially when financial incentives are involved. Some red flags apply universally, no matter who you're recruiting. Others are specific to certain stakeholder groups. Below are four red flags to watch out for across all types of respondents:

1. **Multiple screener submissions from the same person:** Where pre-screening takes place online, watch for multiple survey or screener attempts coming from the same IP address or device, under different names. This can indicate a single individual attempting to figure out qualifying criteria, and in rarer cases, to qualify multiple times to claim several incentives.

2. **An unusual digital footprint:** Fraudulent respondents may use private browsers or VPNs to hide their IP address. A missing IP or one that geolocates to an unexpected country should raise concern. Likewise, VoIP numbers or phone numbers from the wrong region (e.g. non-UK for a UK study) are red flags.

3. **Inconsistent or vague information:** Look for mismatches between names and email addresses, obviously fake names, or vague, off-topic responses to open-ended questions. For example, someone claiming to have a medical condition but offering a generic or nonsensical answer likely lacks genuine experience.

[1] https://www.tremendous.com/blog/market-research-fraud/

4. **Unusual pauses or hesitations:** During phone screening or live qualitative interviews, listen for unusual pauses or hesitations. If a respondent frequently says, “hang on, let me check”, pauses extensively before answering, or gives oddly slow answers to questions, they might be looking up information online to assist with answers.

A note on low quality qualitative responses

Not all short or unenthusiastic answers are signs of fraud. Sometimes, HCPs or patients are just having an off day, feel distracted, or struggle to express their thoughts - and that’s completely normal. Similarly, the interview setting, an unexpected accent, or how someone looks should not be taken as evidence of fraud. If you're unsure about a respondent, it’s fine to reschedule or ask the recruiter to run extra checks. There’s no need to suggest wrongdoing, just say a few things don’t look quite right and you’d like to double-check before continuing, to avoid wasting their time.

For Patients and Consumer Recruitment:

Qualitative studies involving patients or consumers tend to experience higher rates of fraud. It’s easier for someone to falsify a health condition or consumer behaviour than it is to pretend to be a doctor. A patient’s personal health information is private and therefore is not publicly accessible for verification due to strict privacy laws (GDPR). As a result, researchers must rely on what participants self-report in screener questionnaires and interviews - which creates opportunities for fraudulent individuals to slip through. Moderators and recruiters should be alert to certain red flags that may indicate a participant is not genuine, including:

- **Recruiting via public channels**: Be cautious when using general population panels or open social media ads to recruit patients. Fraudsters often lurk in these channels. In contrast, recruits from closed patient communities or advocacy groups tend to be more trustworthy (though not completely immune to imposters).
- **Lack of proof**: For certain studies, you might ask patients to provide evidence of their diagnosis or treatment (for example, the name of a medication, a prescription, or a photo of a pill bottle with their name). A fraudster will often fail to provide adequate proof or give excuses. An outright refusal or an obviously doctored piece of evidence is another red flag.

For Healthcare Professional (HCP) Recruitment:

Fraudulent participation in qualitative HCP research is relatively rare, because it is difficult to convincingly pose as a medical professional. Genuine HCPs have extensive medical training and experiences that are hard for imposters to emulate during an in-depth interview or focus group. However, though uncommon, there have been cases of individuals pretending to be physicians or specialists to take part in studies.

If a fraudster manages to get through the screening process, a skilled moderator can often detect such fraud during an interview – for example, if the person cannot clearly articulate medical concepts or offers treatment opinions that do not align with standard clinical practice. In this instance, it is wise to pause and verify the HCP’s credentials.

Quantitative Research

Quantitative research faces a different set of challenges. As surveys can be taken remotely, they can attract dishonest participants and individuals who deploy technology aiming to game the system.

Fraud in quantitative research spans from individual “professional respondents” who try to take the survey multiple times or speed through for the reward, to organised fraud rings or software bots that auto-complete surveys at scale.

The result of both is corrupted data that can skew findings if not identified and removed. Below are key patterns and indicators to help identify fraudulent entries in quantitative datasets:

Bots and Automated Responses:

The use of bots to fill out surveys has become a growing problem, especially in consumer-focused research with open web panels. Whenever incentives are offered, there is a temptation for respondents to deploy programs that automatically register and complete surveys to claim those rewards. Some bots are highly sophisticated and can mimic human patterns to an extent, but there are often clues in the data that betray them.

One clear giveaway is impossible timing and repetition. For instance, if you observe a batch of completes that all started within seconds of each other or a series of surveys finished in improbably short times (far faster than any human could read and answer), you likely have automated entries. Sometimes the timestamps will reveal a pattern, e.g. the moment one response is submitted, the next one begins, over and over – which is not how independent human respondents would behave. Unnaturally fast completion is a red flag for bot activity.

Open-Ended (OE) Responses and ‘Perfect’ Answers:

Another way to spot fraud in surveys is through open-ended questions. Bots and fraudulent respondents often falter when asked to provide free-text answers that require thought. If your survey contains at least one or two open-ended (OE) questions, review those answers carefully. Extremely generic answers that just restate the question or give irrelevant answers can indicate a respondent who isn’t genuinely qualified or isn’t human. When generative AI is used by fraudsters, they may appear too polished, formulaic or unnatural.

Making Duplicate Survey Submissions:

A common fraud tactic is where one individual attempts to complete a survey multiple times to claim multiple incentives. They might use different email addresses or aliases to register, but often their digital footprint will give them away. Researchers should therefore check for duplicate digital identifiers among completes.

One basic check is looking at IP addresses; if several responses share the same IP address or device ID, it’s likely the same individual (or a coordinated group) attempting to skirt the “one survey per person” rule. However, be mindful: collecting and storing IP addresses is considered personally identifiable information and may raise privacy concerns or violate data protection policies if done without consent. Use this data carefully and in line with regulations.

Some fraudsters are aware of IP checks and use IP masking techniques to avoid detection. They may route their activity through a residential proxy network, which assigns them a real-looking IP address (often associated with an internet service provider in the target country), effectively disguising their true location. This can make a fraudulent overseas respondent appear to be local. In these cases, additional scrutiny is needed – for instance, if other data points (like provided phone number or answers) seem inconsistent with the claimed location, or if the survey uses device fingerprinting technology, it may catch anomalies beyond the IP.

A note on low quality quantitative responses

Although low-quality responses don't necessarily fit the 'fraudulent' category, they can be just as damaging to data integrity as outright fraud. Below are examples of classic patterns to identify:

- **Flat-lining**: When respondents give the same rating or answer for a large set of questions, suggesting they aren't reading the content. For example, if you have a matrix of 20 attitude statements on a 1-7 scale, a flat-liner might just mark "6" for every single statement. One way to catch flat-lining is to include a pair of statements in the grid that contradictory. If a respondent gives high (or identical) agreement to both statements, it is clear they are not paying attention.
- **Speeding:** When respondents complete the survey far too quickly, indicating they skimmed or skipped important content. For example, finishing a 15-minute survey in under 5 minutes. It's good practice when designing surveys to estimate a reasonable completion time and then set a threshold, for instance, to remove anyone who completes in less than 50% of that expected time. In more complex exercises like conjoint analyses or MaxDiff tasks, it can be useful to track the time spent on each task or section. If someone is clicking through complex trade-off questions in seconds, they probably are not giving the responses proper thought.
- **Inconsistent answers**: When respondents give conflicting answers that don't logically align across a survey. For example, stating that they both "never prescribe" and "frequently prescribe" the same drug in different questions, or claiming different specialties or roles in separate parts of the survey.
- **Red-herring responses**: When respondents select an option that is clearly incorrect or implausible, often included deliberately to test engagement. For example, selecting "I prescribe veterinary medications" in a survey for oncologists, or claiming familiarity with a fictitious drug or company.

In summary, spotting fraudulent or poor-quality respondents in quantitative research takes a combination of automated checks and human review. Robust data cleaning and validation serve as the final safeguard against any issues that slip through earlier filters.

The next section outlines how to use technology to catch obvious patterns, and how to layer in manual checks for deeper scrutiny.

Preventing Fraud in Primary Research

While identifying and removing fraudulent data after research has concluded is necessary, it's far more effective to stop fraudsters from entering your study in the first place. This section outlines how to build in safeguards at every stage of the research process, from study design and recruitment through to participation and payment.

A note on working with recruitment partners

If you are working with a panel or vendor to recruit respondents, ask what fraud checks they apply before delivering sample. This might include IP/geo-screening, duplicate detection, behavioural scoring, identity verification or proof of diagnosis - and should be disclosed transparently.

Study Design

Design screeners to be rigorous and less gameable:

The screening questionnaire is your first gateway to keep out ineligible or fake respondents, so it must be well-crafted. Avoid writing screeners that make it obvious what answers will qualify someone; if questions are too leading or use yes/no answers for key criteria, a fraudulent person can easily guess the "correct" answer to get through. Similarly, limit how much information you share about the research study with the respondent prior to the screener being completed, to avoid influencing their responses, introducing bias, or encouraging misrepresentation in order to qualify.

Instead, ask nuanced questions or use multiple-choice options that require specific knowledge. For example, rather than asking "Have you been diagnosed with Condition X? (Yes/No)", you might ask "Which of the following best describes your diagnosis or health condition?" with a list of options that include Condition X among others. This makes it harder for someone without the condition to just say "yes" and get in. Mask the true purpose of questions when possible so that a fraudster cannot tell which answer the "ticket" is to qualify.

Include intentional quality checks in the screener or survey:

Adding a nonsensical or instructed-response question in the screener or survey can filter out both bots and individuals who aren't paying attention. For instance, you can have a question like: "To help us ensure quality, please select the number 10 from the list below" followed by a list of numbers. Anyone who fails to select 10 should not proceed.

Similarly, include a few knowledge or logic checks relevant to the study. If you're recruiting patients with a certain condition, you could ask a basic question about their condition or treatment that a genuine patient would know but an impersonator might not. For HCP recruitment, you might include a question that only a real doctor of the target specialty could answer correctly. These truth verification questions act as tripwires for dishonest respondents.

Similarly, some surveys include a hidden question that isn't visible to the human eye. A human will not know to answer such a question, but a bot, which tries to fill every field, will give an answer. These question-based tricks are simple but effective ways to spot automated or low-effort responses in your data.

Case Study: Geo-Blocking Deters Out-of-Region Fraud

An insights agency took a proactive step to prevent fraudulent and out-of-region respondents by enabling geolocation blocking within their survey platform.

If a respondent's IP address fell outside the study's target countries, they were automatically denied access, significantly reducing "bad" data from opportunistic participants.

The team noted some limitations of geo-blocking. Sophisticated fraudsters can still bypass these blocks by using VPN services or proxy servers that make it appear as if they are within the target country. In fact, someone determined to cheat the system might deliberately point their VPN to an allowed location and still get through. On the flip side, a strict geo-block can occasionally exclude legitimate respondents. For example, a genuine participant who happens to be traveling abroad during the fieldwork period could be blocked from completion. This can be mitigated against by using IA-based IP reputation flagging.

They learnt that while geolocation filters are useful for identifying and preventing obvious fraud, they are not foolproof. These measures must be combined with other checks, and researchers should remain aware of false positives (blocking a real respondent) and have a plan to handle those cases if they arise.

Carefully consider recruitment sources:

As a preventative step, choose recruitment channels that balance reach with reliability. If you use broad online panels or social media ads, implement extra verification steps (covered below) because these sources are open to anyone. If feasible, leverage trusted networks: for example, working with patient advocacy groups to invite members who have been vetted, or using providers who have their own fraud checks and high-quality respondent pools.

In HCP research, consider recruiting via professional networks or lists where credentials have been pre-verified. Additionally, maintain an internal record of individuals suspected of fraudulent behaviour, to avoid inviting them to take part in future research. Cross-checking new recruits against this internal list can help reduce the risk of repeat offenders.

Any such records must be handled in line with GDPR, and care should be taken to ensure only minimal, necessary data is retained. While there's little recourse against individuals committing fraud, especially in organised cases, you can remove their data from the sample, withhold incentives if there is indisputable evidence of fraud, and refrain from future contact. For more detail, refer to the BHBIA's Privacy & Data Protection resources.

Don’t sacrifice the respondent experience:

In tightening your screener criteria, remember that genuine respondents will be going through this process. We are in a highly regulated industry and should communicate the importance of verification. However, if the process is too onerous or feels like an interrogation, you risk turning off the very people you want to engage.

There is a trade-off between fraud prevention and respondent friendliness. Use just a few well-placed quality checks rather than an overwhelming number of traps, and ensure questions still feel relevant and respectful. If a screener is excessively long or peppered with trick questions, even honest participants might drop out due to frustration. Strive for a design that weeds out fraud efficiently without alienating real respondents. After all, a high dropout rate of legitimate participants can hurt your research just as much as letting fraudsters through.

Case Study: Using Personality Metrics to Unmask Bots

An insights and market research agency wanted to ensure that none of their survey responses were being generated by AI.

To test for authenticity, they embedded the Mini-IPIP (a validated psychological instrument that measures the “Big Five” personality traits) into their online survey. Human responses typically follow predictable correlation patterns between traits (e.g., high Conscientiousness often aligns with lower Neuroticism). When they had a bot complete the Mini-IPIP, the resulting trait combinations deviated from all known human patterns.

This provided a clear red flag: any response with an "impossible" personality profile was flagged for further review. By introducing a subtle, psychology-based module into the survey, the team was able to reliably detect and eliminate likely AI-generated responses, ultimately strengthening the integrity of their data.

Identity Verification

One of the strongest ways to prevent fraud is to perform identity verification, especially for high-value research (e.g. qualitative interviews or studies with significant incentives). Identity verification can be done manually or through specialised services and typically involves confirming a participant’s official ID or credentials. In healthcare research, the approach may differ for HCPs vs. patients:

- **HCP Verification**: A common approach is to request a professional registration number (e.g. a UK doctor’s GMC number) and cross-check it against the public medical register. However, since this information is publicly accessible, it’s more robust to also ask for supporting evidence - such as proof of qualifications matching the register, verification of an institutional email (e.g. name@nhs.net), sign-up via a professional address, or employment confirmation through hospital directories.

- **Patient Verification**: Verifying patients is trickier due to privacy, but there are still steps you can take. You might request proof of diagnosis or treatment, such as a doctor's letter or a prescription/medication label that has the patient's name and relevant details. Some research agencies ask participants to show a medication package or appointment letter with their name on it (often via a secure upload or on a video screening call).

  While this can be very effective in confirming someone truly has the condition, be aware of barriers: documents can still be falsified, it's time-consuming, not everyone will feel comfortable sharing such information, and it could slow down recruitment. Use this when appropriate (e.g. non verified recruitment sources such as consumer panels or social media) and always handle any personal health documents with utmost confidentiality. Offering to redact sensitive information, except what's needed for proof, can provide reassurance to participants.

Pick up the phone:

Whether you're recruiting HCPs or patients, a straightforward yet effective fraud check is a phone call verification. A quick call can confirm that the respondent is real, reachable, and matches the profile provided. For instance, reaching a valid number (and speaking to a real person rather than hitting a suspicious voicemail) immediately builds confidence in the respondent's legitimacy. Phone calls also offer an opportunity to validate key screener responses in a natural, conversational way. Fraudsters often struggle to maintain consistency or hesitate when questioned live, making phone verification a useful tool for spotting red flags early.

Consider implementing digital identity verification tools:

In recent years, a range of technology platforms have emerged to automate identity verification, offering a scalable and secure alternative to manual checks. If manual processes aren't feasible, or you're running large-scale or high value studies, integrating an identity verification service into your recruitment workflow can be a highly effective fraud prevention measure. Here's how it typically works:

After a participant qualifies, you send them a secure unique link which opens a verification workflow. They will be prompted to use their smartphone or webcam to capture a selfie or short video of themselves, as well as photos of a government-issued ID (such as a driver's license or passport). This must be completed in one session and within a limited time window.

Advanced facial biometric technology is then used to verify the individual and to check the ID's authenticity. These systems also often cross-reference against databases of known fraudsters or fake IDs, and can even detect if the video/selfie is a recording or deepfake attempt.

The result is a confidence score or pass/fail indicating if the identity is verified. Providers can integrate with survey platforms and CRMs, or can be used on a case-by-case basis. Implementing this adds a robust gate against fake identities and prevents bots or individuals using stolen identities from participating.

Case Study: Automating Expert Identity Verification

A specialist expert network for healthcare research sought to ensure complete trust in the professionals they provide for studies.

They integrated a fully automated identity verification solution into their expert onboarding process. Now, when a new expert (e.g. a physician or specialist) joins their network that meets a certain risk score, that individual must go through an ID verification workflow that checks their photo ID and matches it with a selfie, along with verifying their professional credentials. This process runs seamlessly online and flags any discrepancies or potential fraud (such as someone trying to impersonate a doctor).

By automating this step, the expert network achieved near 100% confidence in the identity of their experts, virtually eliminating the risk of an imposter posing as a thought leader in their network. The result is a highly trusted pool of expert respondents, giving customers peace of mind that experts are genuine and qualified before research begins.

Pick the best time to do it:

There are two logical points to do identity checks: at the start (onboarding or study entry) or before incentives are paid out. Verifying at recruitment stage ensures that only real, verified people enter your study or panel, greatly reducing fraud upfront – but it can slow down fieldwork, so let participants know in advance that this step is part of the process.

On the other hand, verifying identity right before sending incentives can catch anyone who managed to slip through; knowing that payment is contingent on an ID check can also deter fraudsters from even attempting to take part. Some researchers opt for both: a light check at screening and a final confirmation at incentive time, particularly for qualitative interviews where the investment is high. Use identity verification in a way that balances security with practicality.

Balancing results and costs with respondent experience

While identity verification offers strong protection against fraud, it does come with trade-offs, particularly in terms of cost, privacy, and participant experience.

Cost: Most providers charge per check or license fee, so factor this into your budget. For small-scale studies, manual checks may be more affordable.

Privacy: Always get consent before collecting ID documents and ensure compliance with GDPR.

Participant Experience: Some may feel uneasy about ID checks. Clearly explain that it's a standard security step to protect the research integrity. This usually reassures participants.

Fraud Detection Tools and Data Monitoring

Even after recruiting participants, it's critical to monitor for fraud throughout the data collection process. Various tools can automatically detect suspicious behaviour as it happens, and researchers themselves can watch for warning signs in incoming data. Here we cover technical solutions like CAPTCHA and fraud detection services, as well as best practices in survey monitoring:

CAPTCHAs and Bot Filters:

One of the simplest yet effective tools against automated bots is the use of CAPTCHA challenges at the survey start or key entry points. Google's reCAPTCHA, for example, can be integrated into online surveys. Modern reCAPTCHA runs invisibly in the background, assigning a score for how likely the user is human based on their mouse movements and other behaviour. If the risk is high, it might present a challenge (like selecting images or a checkbox "I am not a robot").

By employing CAPTCHA, you can outright block a lot of basic bots from accessing the survey at all. It's a low-effort addition that dramatically reduces spam entries. Some survey platforms have built-in CAPTCHA options or you can script one in. Keep in mind that CAPTCHAs aren't foolproof (advanced bots can sometimes solve them, and they don't stop human fraudsters), but they are a valuable first line of defence.

Specialised Fraud Detection Services:

There are dedicated services (such as IPQualityScore, RelevantID, Imperium, Research Defender, and others) that integrate with surveys or panels to catch fraud in real time. These tools analyse a variety of signals: a respondent's IP address and geo-location, device fingerprint (browser, OS, device type), behavioural patterns (like keystroke dynamics), and even email/domain reputation. Using machine learning and huge databases of known fraudulent data points, they assign a risk score to each entry.

If an entry is flagged (for example, the IP is known to be from a VPN or has been associated with past fraud, or the device is showing signs of automation), the system can automatically prevent the respondent from continuing or mark the data for follow-up. Some panels use these systems in the background, so if you're working with a panel company, ask what fraud detection measures they have; they might already be filtering out high-risk respondents so you never see them.

For your own surveys, these solutions can often be added via an API or as an extension of your survey platform. The benefit of automated fraud detection is speed and thoroughness – it can check every respondent against thousands of risk factors far faster than any human could.

Real-Time Data Monitoring:

Even with automated tools in place, researchers should actively monitor survey data during fieldwork. Most online survey platforms (Qualtrics, Decipher, Forsta, etc.) allow you to view incoming results and often include some built-in quality checks. Set up alerts or periodically check for things like very fast completes, an unusual spike in completes at odd hours, or any identical patterns in answers.

If your platform has a feature to flag straight-lining or inconsistent answers, make sure it's enabled. Some platforms can enforce rules (e.g. automatically screen out anyone who completes under a certain time, or who fails a trap question). Use those features to stop bad data early, rather than only cleaning it at the end.

For qualitative research, if you're conducting online interviews or focus groups, monitoring might involve verifying that the people who show up to the session match who was recruited (e.g. do a quick ID check at the start of a webcam interview if needed). If anything feels off during an interview, it's better to cut it short than to continue with questionable data.

Additional technical safeguards:

Consider other small technical tweaks that can discourage fraudulent activity. For example, you can disable copy-paste functionality in the survey to prevent respondents from easily copying answers (or from pasting in pre-prepared text, which some professional cheats might do to answer open-ends or knowledge questions). Another measure is using tools like reverse image search or metadata checks on any files respondents upload. This could verify if a photo provided as "proof" is original or something lifted from the internet.

While such methods may not be standard for all studies, they can be useful in specific cases (for instance, if you ask for a photo of a medical device the patient uses, a quick reverse image search on what they send can tell you if that image is appearing on some stock photo site or forum, indicating it's not genuinely theirs).

Balance automation with human oversight:

Automated fraud detection will catch a lot, but it can also produce false positives. For instance, a legitimate respondent might inadvertently appear suspicious (i.e. using a VPN for valid reasons, or a fast reader who completes quicker than average but still answers conscientiously). It's important not to blindly purge all "flagged" respondents without a secondary review.

Build in a step to manually review borderline cases. If a respondent is flagged for speed but their answers look thoughtful and consistent, you might keep them. Conversely, if someone passes automated checks but something in their open-ended responses feels off, trust your research instincts and investigate further. The best outcome comes from using technology to cast a wide net and then using researcher judgment on the catch.

A note on implementing anti-fraud solutions:

Not every team has the resources for round-the-clock oversight or complex deployments. When planning your approach, match your fraud prevention strategy to your budget and capabilities. Even simple, low-cost tactics like trap questions, manual data reviews, and re-checking respondents before every survey, can make a meaningful difference.

Ensure any solutions integrate smoothly with your existing systems to avoid operational issues. And always stay compliant with data protection regulations, e.g. if you're logging IP addresses or using device fingerprinting, update your privacy notice accordingly and limit data use strictly to fraud prevention.

In essence, preventing fraud in research is about creating multiple checkpoints: a strong screener to keep the obvious fraud out, identity verification to ensure people are real, and ongoing technical and human monitoring to catch any sneaky behaviour. Each project might require a tailored mix of these strategies. By deploying them carefully, you can reduce the incidence of fraudulent respondents, maintaining the quality and credibility of your findings.

Conclusion

Fraudulent respondents undermine the integrity of healthcare market research, but with the right approach, they can largely be prevented. In qualitative studies, vigilant recruiters and moderators are key; in quantitative work, well-designed surveys and detection tools help filter out bots, duplicates, and low-effort responses.

For pharmaceutical companies, the stakes of poor data quality are high. Whether it's early-stage market landscaping, message testing, or evaluating patient pathways, decisions are made based on primary research findings. If fraudulent respondents infiltrate the data, the consequences can ripple through commercial strategy, regulatory submissions, and more.

This makes fraud prevention not just a research concern, but a **business imperative**. Trustworthy research starts with trustworthy participants. While detection tools play an important role, human oversight remains essential. By investing in layered protection across people, process, and platforms, researchers and their clients can protect data integrity and maintain confidence in their insights.

About the BHBIA and the Fieldwork Committee

The British Healthcare Business Intelligence Association (BHBIA) is the professional association for organisations and individuals involved in UK healthcare market research and business intelligence. Within the BHBIA, the Fieldwork Committee focuses on enhancing the quality and integrity of fieldwork activities. This guide has been developed by the Fieldwork Committee to help BHBIA members identify and prevent fraudulent respondents in primary market research.

View Fieldwork Committee members here

Disclaimer

British Healthcare Business Intelligence Association
St James House, Vicar Lane, Sheffield, S1 2EX
t: 01727 896085 • admin@bhbia.org.uk • www.bhbia.org.uk
A Private Limited Company Registered in England and Wales No: 9244455

BHBIA

Appendix

Glossary of Terms

Term	Definition
Bot	A software programme that automatically completes surveys and screeners without human input.
Device Fingerprinting	A technique that tracks specific device characteristics (browser type, screen resolution, etc.) to uniquely identify users.
Duplicate Submission	When an individual attempts to complete the same survey or screener more than once, either to claim multiple incentives or boost response counts. This may involve different email addresses, IP addresses, or devices.
False Positive	When a legitimate respondent is mistakenly flagged as fraudulent by a detection system.
Flatliner (Quant)	A respondent who selects the same answer repeatedly across multiple questions, indicating disengagement or low effort.
Generative AI Response	A response generated using tools such as ChatGPT, Claude, Grok or Gemini.
High Speeder (Quant)	A respondent who completes a survey significantly faster than expected, suggesting they may not have read or considered the questions properly, or may not be a genuine respondent at all.
IP Masking	The act of hiding or altering a device's IP address to obscure identity or location. Often used in combination with proxies or VPNs.
Private Browser	A browsing mode (such as 'Incognito' in Chrome) that doesn't store cookies or history, often used to bypass screening mechanisms or appear as a 'new' respondent.
Proxy Network	A method used to disguise a respondent's true location by routing internet activity through different residential IP addresses.
Synthetic Respondent	A respondent who may either be fabricated, impersonating a real person, or created using AI.
Trap Question	A survey question with a clear 'correct' answer, designed to identify inattentive or bot respondents (e.g. "For quality control, please select option 3").
VoIP (Voice over Internet Protocol)	A technology that routes calls over the internet. Can be used to hide a respondent's true location or identity.
VPN (Virtual Private Network)	A privacy tool that masks a user's location by re-routing their internet connection through a server elsewhere.