Intellus Worldwide Data Integrity Committee

Fraud Prevention CHECKLIST

Michael Wildt
Owl Solutions

Isabelle Davoudiasl
EXAFIELD

Data Integrity Committee Co-Chairs

Scan for more DI Resources

FRAUD-PREVENTION CHECKLIST GUIDELINE

High-quality data is essential in healthcare market research, but increasingly sophisticated fraud (such as identity spoofing, fake or stolen credentials, duplicate accounts, coordinated bad-actor networks, and bot-generated responses) threatens respondent authenticity and data integrity.

This checklist supports manufacturers and insights providers by highlighting key anti-fraud and identity-verification measures used by panel providers, recruitment partners, and software programmers.

It forms part of the broader work of the Intellus Data Integrity Committee and the GDQ Pledge, both dedicated to establishing practical guidelines that strengthen fraud prevention and data integrity across healthcare research.

Purpose of This Checklist

- Provide a standardized set of questions to ask insights providers and panel providers about their fraud-prevention and identity-verification processes.
- Help buyers assess at the RFQ stage whether a supplier meets minimum expectations for respondent quality.
- Encourage transparency into the technical, behavioral, and manual controls used by vendors.
- Reduce exposure to fraudulent or low-quality data by leveraging multiple complementary safeguards rather than relying on a single method.
- It is understood that each organization may apply its own judgment, priorities, and risk tolerance. This checklist is meant to inform decision-making, not replace it.

How to Use This Checklist

1. Manufacturers to include the checklist in RFQ or onboarding package for all Insights Providers, who will be tasked with obtaining this information from panel/recruitment/programing suppliers for comprehensive assessment.

2. Request vendor responses using the YES/NO format with supporting detail.

3. Review answers internally and flag NO responses in critical high-risk areas.

4. Use the responses to guide supplier discussions and qualification decisions.

5. Please note that some questions in this checklist are primarily directed toward panel providers/recruitment partners, while others are more applicable to programming teams or software/platform partners.

Vendor Name:

Project Number:

Sample Vendor Checklist

Does sample provider validate real identity before granting panel access? (email, SMS OTP, ID verification, third-party tools)	
Does sample provider verify HCP credentials (NPI, medical license, specialty) and revalidate periodically?	
Do they scan and detect high-risk IPs, VPNs, proxies, and datacenter traffic at signup?	
Are respondents recruited using open-source recruiting? (Social media platforms, forums, etc.)	
If CATI is method is used, will all the recording be available to review?	
Is your sample provider and insights provider a GDQ pledge signee?	

PRE-Survey Checklist

Is ReCaptcha or equivalent, being used?	
Is Digital Fingerprint enabled? *Research Defender, Clean ID, DeviceForens/Q, Relevant ID, or proprietary*	
If yes, will all possible entrants that fail a predetermined fraud score be terminated before entering survey?	
Does your digital fingerprint solution use Cross-Panel Monitoring to stop duplication? or	
An internal suppression list, flagging bad actor after 1st offence? or	
3rd party monitoring of Fraud Databases & Blacklists?	

IN-Survey Checklist

Use automated tools to detect data entry patterns, on-screen translators, response patterns, or logical consistency?	
Use automated tools to evaluate open-end responses for AI-generated answers, Wrong topic, Wrong/Bad language, Duplicates, Poor quality, copy paste?	
Use behavioral analytics tools that measure mouse activity, keystroke dynamics, and navigation patterns?	
Are bot traps being programmed into the survey, with suspected fraud completes flagged in the data file?	

POST-Survey Checklist

Is a 3rd party payment vendor being used to validate respondents' payment	
Is yes, are new members restricted from redeeming incentives until they meet quality thresholds?	
Are manual fraud and quality checks being done by insights provider?	