



FOILING CHEATERS, BOTS & AI-GENERATED RESPONSES

Strengthening Data Quality in a Changing Research Environment

Since we first published our *10 Expert Tips for Foiling Cheaters and Bots*, the fraud landscape has evolved dramatically.

What began as speeders, copy-paste responses, and obvious bots has matured into AI-generated open-ends, masked digital fingerprints, coordinated fraud rings, and increasingly sophisticated automation.

Data quality is no longer about catching careless respondents. It's about staying ahead of adaptive systems.

BELOW IS OUR UPDATED FRAMEWORK FOR PROTECTING SURVEY INTEGRITY TODAY.

TIP #1:

OPEN-END PROTECTION NOW REQUIRES AI AWARENESS

Open-ends remain one of the strongest fraud detection tools, but they now cut both ways.

What's new:

- AI can generate coherent, grammatically correct responses instantly.
- Bots can now simulate human typing delays and keystroke patterns.
- Copy/paste detection alone is insufficient.

Our recommendations:

- Disable copy/paste functionality where appropriate.
- Monitor typing speed patterns such as characters-per-second and time-to-first-response.
- Flag uniform sentence structures and overly polished language.
- Look for context misalignment (responses that sound good but don't answer the question).
- Combine automated AI-detection tools with human review.

TIP #2:

HUMAN REVIEW IS MORE IMPORTANT THAN EVER

AI may produce polished answers, but it often lacks lived context, emotional specificity, or internal consistency.

We continue to:

- Review open-ends during field, not just at close.
- Cluster or sort open-end responses to detect repeated phrasing patterns.
- Identify repeated misspellings or phrasing clusters.
- Look for internal contradictions across responses.
- Evaluate tone consistency across multiple open-ends.



TIP #3:

SCREENER DESIGN MUST ANTICIPATE STRATEGIC FRAUD

We design screeners by thinking like a cheater so we can stay ahead of them.

Suggested best practices:

- Funnel-based design to mask qualification criteria.
- Inconsistent but logical cross-check questions.
- Delayed terminations to obscure qualification triggers.
- Designing screeners that require experiential knowledge rather than obvious desirability.

TIP #4:

DIGITAL FINGERPRINTING IS NECESSARY BUT NOT SUFFICIENT

Protecting data integrity today demands an integrated, multi-layered monitoring approach.

Modern bad actors:

- Mask IP addresses.
- Rotate IPs and browser/device signatures.
- Use VPNs and device emulators.
- Manipulate browser environments.

We recommend:

- Behavioral fingerprinting.
- Device and browser consistency checks.
- Pattern recognition across completes.
- Ongoing source performance monitoring.

TIP #5:

MOBILE-FIRST ENVIRONMENT = NEW FRAUD PATTERNS

The majority of surveys are now completed on mobile devices.

Mobile introduces:

- Different timing patterns.
- Higher multitasking behavior.
- Increased bot experimentation.

As such, speed and behavior should be evaluated in context, adjusting thresholds to reflect device type and survey complexity. Thoughtful limits will protect your data quality without removing legitimate respondents.

TIP #6:

DEFINE "SOFT STRIKES" VS. AUTOMATIC TERMINATIONS

Because not every anomaly equals fraud, overcorrection can be as damaging as under-detection.



A sophisticated data quality approach should:

- Distinguish between inattentiveness and automation.
- Assign weighted behaviors.
- Establish termination thresholds.
- Avoid over-cleaning that introduces bias.

TIP #7:

CAPTCHA & BOT TOOLS: PART OF THE STACK, NOT THE STRATEGY

CAPTCHA technologies (text-based, image recognition, behavioral, invisible) and honeypot traps, however:

- Bots are increasingly trained to bypass traditional CAPTCHAs.
- CAPTCHA friction can impact legitimate respondents.

We recommend using CAPTCHA tools as one layer of defense, supported by behavioral analytics and active oversight.

TIP #8:

AI HAS CREATED A PARADOX

We now use AI tools to:

- Analyze open-ends.
- Detect patterns.
- Identify anomalies.

At the same time, respondents use AI to:

- Generate responses.
- Evade detection.
- Produce consistent but hollow narratives.
- Produce overly structured or generic narratives.

This results in a continuous game of advancement and countermeasure. Which is why layered methodology, not a single tool, is necessary for effective data protection.

TIP #9:

READ DURING FIELD, NOT JUST AFTER

Because not every anomaly equals fraud, overcorrection can be as damaging as under-detection.

In-field monitoring allows us to:

- Catch quota contamination early.
- Adjust sample sourcing.
- Identify emerging patterns before close.
- Prevent costly re-fielding.



TIP #10:

DATA QUALITY IS AN ONGOING DISCIPLINE

The challenge of cheaters and bots has become a constant presence in online research. Methods that were effective just a few years ago remain valuable, but today's environment requires deliberate design, active monitoring, and ongoing protection.

We recommend a modern approach that includes:

- Technical safeguards
- Behavioral analytics
- AI awareness
- Human oversight
- Continuous refinement

THE BOTTOM LINE

Fraud is smarter. Automation is faster. AI is more accessible.

Which means protecting data quality today demands vigilance, layered safeguards, and experienced oversight. Strong insights are built on carefully designed protections that leverage the right combination of technology, behavioral intelligence, and expert judgment to stay ahead of evolving threats.

At Research Results, data integrity sits at the center of everything we do. We bring the tools, experience, and disciplined oversight needed to safeguard every study. If protecting your data is a priority, we would welcome the opportunity to partner with you.

In addition to these strategies and tools for catching cheaters and bots, Research Results has developed proprietary tools, including RADAR™, our quality framework designed to strengthen respondent validation and help protect data quality before responses enter a study.

Also, we've included our Cheater and Bot Taxonomy below to help you stay up-to-date with the evolving respondent threats.

If you'd like to learn more about contact

Ellen Pieper, Chief Client Officer, Ellen_Pieper@researchresults.com, or 919-368-5819 today!



Cheater and Bot Taxonomy

Market researchers must remain vigilant against evolving respondent threats. While traditional fraud types remain relevant, advances in AI, automation, and organized networks have introduced new complexities.

- **Slackers** are inattentive respondents who rush, straight-line, or provide low-effort answers. While not always malicious, they compromise data quality through disengagement.
- **Professional survey farms** employ individuals to complete high volumes of surveys daily. Their focus is completion and incentive capture rather than thoughtful participation, and many coordinate to avoid detection.
- **Over-reporters** misrepresent behaviors, qualifications, or expertise to gain entry into surveys, often studying screeners and adjusting answers strategically. This may include exaggerating socially desirable behaviors or claiming responsibilities they do not actually hold.
- **Technical manipulators** alter survey links, mask devices, rotate IP addresses, or attempt to generate fraudulent completes while concealing digital fingerprints.
- **Bots** are automated programs built to complete surveys. Modern bots increasingly mimic human timing, mouse movement, and typing cadence to evade detection.
- **AI-assisted respondents** use generative AI tools to craft polished open-end responses that appear coherent but lack authentic lived context.
- **Coordinated fraud actors (fraud rings)** share qualification criteria and survey strategies within private groups, making detection more difficult at the individual level.
- **Overly optimized respondents** attempt to mirror “ideal” answering behavior, providing uniformly positive, patterned, or strategically consistent responses designed to avoid removal.
- **B2B impersonators** misrepresent their professional identity, job role, or company affiliation in order to qualify for business or professional research studies. They may claim senior titles, specialized expertise, or decision-making authority they do not actually possess, often adapting their answers during screening to align with perceived qualification criteria.