Why We Say Yes When We Doubt

Trust, Social Pressure, and Independent Judgment as AI Changes Scams

Allie Myerson

Founder, Tech Talk for Seniors

October 2026

Suggested citation: Myerson, A. (2026). Why we say yes when we doubt: Trust, social pressure, and independent judgment as AI changes scams. https://doi.org/10.2139/ssrn.7611958

This work is licensed under a Creative Commons Attribution 4.0 International License (CC BY 4.0).

Abstract

Why can a request feel suspicious and still be difficult to refuse? Drawing on published research and my experience with Tech Talk for Seniors, this paper examines how emotion, social expectations, and the desire to help can lead people to comply despite their doubts. Artificial intelligence (AI) makes personally tailored messages easier to produce, increasing the importance of understanding what makes them persuasive. During short, high-pressure encounters, scammers can push people to act now, keep quiet, and check only through channels the scammer provides; I examine each as a point where that pressure might be resisted. A central insight is that people can step away and verify a request independently, even when they are unsure whether it is fraudulent. The paper connects this practical approach to a broader human question: how can support help people exercise their own judgment while preserving trust and independence?

Keywords: *fraud susceptibility; impersonation scams; scam prevention; persuasion; help-seeking; older adults; social influence*

Key takeaways

1. **Scams are not only an older person's problem.** Relative to their numbers, adults aged 18 to 59 report losing money to fraud more often than older adults, though older adults who lose money report higher median losses. Feeling confident you can spot fraud is not the same as being safe.
2. **Doubt is not the same as saying no.** People can sense that something is wrong and still feel responsible for helping, cooperating, or acting quickly.
3. **You do not need to spot AI, or prove a caller is lying, before you check.** AI can make a message feel personal, but accurate details do not make a request genuine. Ending the exchange and contacting the bank or a relative through a number you already have is a reasonable step, though the specific guidance proposed here has not been tested.
4. **If someone you love has been scammed, start with what they fear losing.** It may not be embarrassment. It may be independence. Afterward, people need to know what to do next, not only what they could have done differently.

Debby's experience: The starting point for my inquiry

When Debby told me about a banking scam she had fallen for, she recalled feeling embarrassed and angry with herself. At the time of the scam, she had worried that telling her children would make them question her ability to live independently. I tried to reassure her that younger people fall for scams, too. I soon realized I was addressing her embarrassment, not the fear of losing her independence that she was describing.

Debby is a 90-year-old retired psychologist whom I met through Tech Talk for Seniors (techtalkforseniors.org). I founded the program in ninth grade after watching my grandfather struggle with technology in his nursing home. Residents of the senior community where we meet bring questions about finding a photo, sending a message, or changing a setting. Helping them use devices to stay connected and independent has also taught me to reconsider what I find obvious.

Hearing about Debby's hesitation to tell her children about the scam raised a question I had overlooked: what might asking for help cost? An effort to protect her could also threaten the independence she wanted to preserve.

I became interested in similar questions during summer courses on AI and the psychology of social media. Why does the same message draw one person in while another passes over it? How do businesses and social expectations shape that response? These questions connected my interests in psychology, technology, and business to sociology: understanding people within the relationships and institutions around them.

Scams raise the stakes of those questions. A request can appeal to someone's sense of responsibility to a family member, an employer, or an institution, making a response feel like a duty. That raises a practical question: what would help someone pause and check a request independently, even when they feel pressure to respond?

Scope and approach

This paper brings together a review of research relevant to these questions and my experience with Tech Talk for Seniors. It focuses on brief encounters in which someone feels pressured to act on an unexpected request for money or sensitive information. Prolonged manipulation and situations in which another person already controls someone's finances are beyond the scope of this paper.

The studies and reports measure different outcomes, including reported losses, what people say they would do, whether they click a link, and how they describe their experiences. Throughout the paper, I distinguish their findings from my interpretations and proposed responses. My conversations through Tech Talk reflect individual experiences and cannot represent everyone's experience with scams. Debby's account reflects my recollection of our conversation; whether AI was involved in her scam is unknown. The appendices document the sources and the selection approach.

Looking beyond age

In March 2026 congressional testimony, the Federal Trade Commission reported approximately three million fraud reports for 2025 and $15.9 billion in reported losses (Federal Trade Commission [FTC], 2026a, p. 2). These figures show the scale of reported harm, but they do not establish how much of that fraud involved AI.

The FTC's separate analysis of 2024 reports shows why age comparisons require care. Relative to population size, adults aged 60 and older reported losing money to fraud at a lower rate than adults aged 18 to 59. When they did report losing money, however, their median losses were higher than those of every age group under 60: $900 for adults aged 60 and older and $1,650 for those aged 80 and older. Age was available in about 45% of fraud reports. The FTC identifies both differences in avoiding loss and differences in reporting as possible explanations for these patterns (FTC, 2025b, pp. 18, 21-22).

These patterns do not tell us who would be more likely to fall for a scam if everyone faced similar requests. They show why an inquiry that began with my work with older adults needed to look beyond age.

Confidence is also an incomplete guide. In a probability-panel survey of 1,004 U.S. adults conducted in September 2025, 71% expressed confidence in detecting financial fraud. In a separate question, 63% said they would definitely or probably invest in a hypothetical offer promising a guaranteed, risk-free 25% annual return for five years. Those percentages do not reveal how many respondents gave both answers (Fontes et al., 2026, pp. 3-4, 8).

This makes me reflect on my own comfort with technology. Being familiar with devices does not tell me how well I would judge an unfamiliar request. To understand that decision, I need to look more closely at the encounter itself: what is at stake, who appears to be asking, and why responding might feel important.

Credibility and the pressure to act

What the request seems to mean

A demand for money might appear to offer a way to protect an account, help a relative, or obtain work. Following instructions could then feel like the careful or responsible thing to do. Before asking why someone would fall for a scam, it helps to ask what they believed responding would accomplish.

DeLiema and colleagues examined survey data from 1,375 U.S. and Canadian consumers who had reported scams to BBB Scam Tracker. Financial fragility was associated with losing money in opportunity-based scams, which promise a gain, but with a lower likelihood of responding to threat-based scams, which warn of a loss or penalty. Perceiving a person or organization as official was associated with loss in several categories. These are associations among selected reporters, and responding is a different outcome from paying (DeLiema et al., 2022, pp. 1, 3-4).

These findings suggest that financial pressure can matter differently depending on the request. Someone may have different reasons for responding to an offer that promises to improve their finances than to a threat to money they already need. The report also connects apparent authority with the source credibility used in legitimate marketing (DeLiema et al., 2022, p. 5). That connection helps explain why businesses matter to this question. An impersonator can borrow a business's name and familiar ways of communicating to make a request seem trustworthy.

Doubt and obligation can coexist

Believing a claim and feeling compelled to act on it deserve separate attention. Chanenson and colleagues analyzed 405 selected English-language Reddit posts about seeking help with financial scams. Their analysis of these self-reported experiences describes accounts in which wanting to be helpful coexisted with suspicion, and others in which financial need contributed to proceeding despite perceived risk (Chanenson et al., 2026, sections 3.3, 3.5, 4.1.2, and 4.3.1).

One charity-scam account describes someone who suspected deception but worried that refusing a genuine appeal could abandon a person in need (Chanenson et al., 2026, section 4.1.2).

This suggests that noticing a warning sign may be only part of the decision. What might refusing the request mean to the person receiving it? When a caller claims a family emergency, questioning them could seem inconsistent with being a caring relative. When someone appears

to represent an official agency, ending the exchange could feel like refusing to cooperate. A person may have doubts and still feel responsible for responding.

Those feelings of responsibility connect the individual decision to a wider social setting. A parent, employee, customer, or friend may feel different obligations when faced with the same request. Whose authority we accept, what we consider polite, and whom we feel comfortable asking for help are shaped by our relationships and communities. Understanding how those expectations vary across cultures would require further research.

Emotion during the encounter

A person's response can also depend on how they feel during the exchange. Researchers use "emotional arousal" to describe how emotionally activated someone feels. High arousal can involve excitement or fear, while low arousal is a calmer state.

Kircanski and colleagues experimentally varied emotional arousal before adults evaluated misleading advertisements. Among participants who showed the intended arousal response, high positive and negative arousal increased stated purchase intention relative to low arousal. The effect was significant within the older group; the difference in the effect between age groups was not significant (Kircanski et al., 2018, pp. 329-334).

The inclusion of positive emotion matters. An apparent opportunity can inspire excitement or hope, just as a threat can create fear. This finding suggests that understanding a decision means paying attention to emotions that feel welcome as well as those that feel uncomfortable.

Urgency, isolation, and control of the exchange

Alongside those feelings, the conditions of an exchange can shape how much room someone has to question a request. For the pressured encounters at the center of this paper, I focus on three questions: must the person act immediately, is independent discussion being discouraged, and does the supposed check remain under the caller's control? In everyday terms, the pressure is to act now, keep quiet, and check only through channels the scammer provides. I use these questions to organize the evidence, not to suggest that every scam requires all three conditions.

A published case makes the combination concrete. In a study of 17 scam reporters, Honick and colleagues describe Jackie, a 19-year-old identified by a pseudonym, who followed an apparent tax authority's instructions to buy gift cards while staying on the phone and telling nobody. The authors connect the encounter with authority, compliance, and fear of appearing ignorant (Honick et al., 2021, pp. 1, 14).

These conditions can reinforce one another. A deadline leaves less time to reconsider. Secrecy keeps another perspective out of the conversation. Staying on the caller's line gives that person the chance to answer each doubt and direct the next action. Interrupting one of these conditions may create room for a different decision, but what happens next matters. Waiting briefly and then following the same instructions still leaves the underlying claim unchecked.

A survey of 1,408 BBB Scam Tracker reporters found that, among those who engaged with a solicitation, having nobody available to discuss it with and choosing not to discuss it were each associated with losing money. This association does not show that discussion itself prevented loss (DeLiema et al., 2019, pp. 2, 12).

Being alone, being told to keep a secret, and deciding not to ask someone for help are different circumstances. Debby did not seek help during the scam. After recognizing what had happened, she was able to resolve it with her bank, but she had worried about telling her children. Her

account does not establish why she did not seek help during the scam. It does show that seeking practical help from an institution and sharing the experience with family can involve different concerns. Telling family, participating in a study, and filing a fraud report also involve different audiences and reasons for speaking up.

Those differences matter when interpreting research. A study that recruits through scam reports begins with people who chose to tell that service what happened. Their accounts cannot tell us directly about people who never reported. Those missing experiences limit the conclusions we can draw.

What a check actually establishes

Even when someone seeks help, the answer may not resolve the question that matters.

In the interview report by Honick and colleagues, Karl described checking with his bank that a deposited check had cleared before sending money onward. The check later proved fraudulent (Honick et al., 2021, pp. 17-18). The FTC explains the underlying distinction: deposited funds may become available before a fake check is discovered (FTC, 2025a).

Karl's account shows why "ask someone" may be incomplete advice. He contacted a legitimate institution, but the answer he described did not establish whether the transaction was genuine. A response can be reassuring without verifying what the person needs to know. A useful check must address the claim behind the requested action, rather than a related fact that leaves that claim unresolved.

What AI changes

AI matters here because it changes the production of deceptive material. In a fraud advisory, the FBI describes criminal use of generated text, images, audio, and video. Such tools can reduce the effort of impersonation and remove some familiar warning signs, including awkward language (Federal Bureau of Investigation [FBI], 2024).

Czybik and colleagues provide more direct evidence about personalization. In a field study involving 7,741 university employees, publicly available information was used to tailor phishing emails. AI-personalized messages produced higher click rates than generic messages, while a smaller manually personalized comparison performed better still. The setting was institutional awareness training, and the outcome was clicking a link, not surrendering credentials or money (Czybik et al., 2026, sections 5-6 and 8.2).

What stands out to me is how AI can make it easier to connect a message to someone's life. Available details can help shape an appeal around what a person cares about or feels responsible for. This connects AI to the earlier question of what a request seems to mean to the person receiving it.

Stolen data adds another possible source of that relevance. Europol describes illicit data markets and AI-assisted tailoring of social engineering. Together with the phishing study, this supports the concern that accessible personal information can be incorporated into persuasive requests (Europol, 2025, pp. 4, 6, 11, 14; Czybik et al., 2026).

A message can include accurate personal details without making its request trustworthy. Contacting the person or organization independently offers a way to check the request without first having to determine whether AI produced it. The question, then, is what helps someone take that step during a convincing exchange.

Making independent judgment easier to exercise

The FTC's advice includes the instruction to "Resist the pressure to act immediately." It also recommends contacting an organization through a trustworthy route and discussing an unexpected request with someone trusted (FTC, 2023). Building on that guidance, I consider what might help someone put it into practice. The language and support practices below are proposals to evaluate, rather than approaches this paper has shown to be effective.

During an uncertain encounter

For an unexpected request involving money or sensitive information, a person can end the incoming exchange before taking the requested action, then contact the organization or person through a previously established route. In a banking scenario, the check should address both the alleged account problem and the proposed transfer. In a family scenario, it should address the person's situation and the payment request. A number or referral supplied by the incoming caller can leave the inquiry inside the same deception (FTC, 2023; FBI, 2024).

These steps address the urgency, isolation, and control discussed earlier. Ending the exchange gives someone room to think outside the caller's timetable. Talking with another person can bring in a different perspective. Making independent contact allows someone other than the caller to confirm or question the request. Each step may create an opportunity to reconsider, but taking a step does not necessarily resolve the uncertainty. An unanswered call leaves the request unverified. A helper who accepts the caller's story without checking it may offer reassurance without confirming that it is true.

Simple phrases can make the next step easier to express: "I need to check this first," or "I will contact them myself." They give someone a way to end the exchange without having to accuse the caller of dishonesty. The aim is to make an independent check possible, not to prescribe a fixed waiting period. If there is a genuine emergency, the person still needs to seek appropriate help through an independent source.

Checking can also provide a reason to trust a request. If it is verified, the person can resume contact and decide how to respond. Someone can take another person's needs seriously while choosing how to confirm what is being asked.

After someone has acted

The response must change when an incident has already occurred. Chanenson and colleagues distinguish four help needs (sensemaking, guidance, therapeutic support, and external action) across stages of a scam (Chanenson et al., 2026, section 4.2). Someone asking for help afterward needs to know what they can do next, rather than only what they could have done differently.

Where money has been sent, the FTC recommends promptly contacting the relevant bank or payment provider, explaining the fraud, and asking about reversal or recovery. Recovery is not guaranteed (FTC, 2026b). A family member can offer help with that process while asking how the person wants them to be involved. Looking back on my conversation with Debby, I would begin by trying to understand her concern about telling her children, without assuming they would respond as she had feared.

The role of organizations and communities

Banks, platforms, and educators also shape the choices available to someone facing an uncertain request. The earlier discussion raises practical questions about the guidance they provide: does a warning explain what to do next? Can the person reach someone

independently? Is it clear what that contact can verify? A bank could examine whether customers understand the difference between funds being available and a check being genuine. A community program could ask whether people feel able to follow its advice when a caller sounds authoritative.

The people receiving that guidance should help evaluate it. My work with Tech Talk has taught me to pay attention to what a resident wants to accomplish, and Debby helped me recognize a concern my reassurance had missed. Listening in the same way could help organizations understand what makes their advice useful or difficult to follow. Responsibility is shared: people need practical ways to check a request, and organizations have a role in making those options clear and accessible.

Limits and a question for further research

The studies and reports examine different groups of people and different outcomes, so bringing them together does not establish a single explanation for why scams succeed. Several focus on particular English-speaking groups. Their findings cannot establish how experiences differ across cultures or what happened to people who never reported a scam. Urgency, isolation, and control help organize the encounters discussed here, but they do not describe every form of fraud. The language and support practices I propose have not been tested for effectiveness.

A research committee of the Federal Trade Commission's Scams Against Older Adults Advisory Group (2024) found "relatively little research directly testing the efficacy of scam-prevention messaging" (p. 2) and listed, as an open question, which actions most reduce risk (p. 10). One field experiment shows that such advice can be tested against real responses: a warning call made prior fraud victims less likely to fully accept a staged scam call, although the effect of a warning about the same scam was no longer detected at four weeks (Scheibe et al., 2014). A study would therefore also need to measure how long any effect lasts.

A future study could compare standard warnings with guidance that explicitly tells people they can end an exchange and gives them an independent way to check the request. It could examine whether participants actually end the exchange, make independent contact, and get an answer that addresses the claim behind the request. It could also assess their willingness to seek help. The study would need to protect participants from real financial harm.

Returning to Debby

Debby helped me understand why support needs to take a person's concerns about independence seriously. She had worried that telling her children about the scam would change how they viewed her ability to manage her own life. My reassurance that younger people are deceived too had left that concern unanswered.

The research helped me see a related difficulty during a scam: someone can doubt a request and still feel responsible for responding. AI can make an appeal easier to personalize, while urgency, isolation, and the caller's control can make it harder to question. Understanding those pressures means looking beyond whether someone recognized a warning sign to whether they felt able to act on it.

In my ongoing work with Tech Talk, I want to better understand what helps someone move from doubting a request to checking it independently. The simple phrases I suggested for ending an exchange remain proposals; whether they help someone take that step has not been tested. Debby's experience reminds me to listen for what someone fears losing or feels responsible for, since those concerns may make practical advice difficult to follow. What I take from this research is that uncertainty is reason enough to verify a request independently.

Acknowledgments

I am grateful to Dr. Elaine Johnson, whose *Psychology of Social Media* course at Emory Pre-College helped me see the connections among my interests in psychology, technology, and business. She introduced me to the possibilities of independent research and encouraged me to pursue questions beyond the classroom. Her course left me curious about why people respond differently to the same messages, a question that eventually helped lead me to this paper.

I want to thank Debby for trusting me with her story and allowing me to share an experience that was deeply personal. Her honesty helped me recognize questions I might not otherwise have thought to ask.

Finally, I am grateful to the residents of Tech Talk for Seniors, who have taught me as much as I have tried to teach them. Their openness and perspectives continue to challenge my assumptions and deepen my understanding of the people behind the technology.

About the author

Allie Myerson is a native New Yorker with a strong interest in the intersection of technology, psychology, and human behavior. She is particularly curious about how technology influences communication, decision-making, and social relationships. As the founder of Tech Talk for Seniors, a volunteer initiative that helps older adults navigate technology with greater confidence and independence, Allie has seen firsthand how trust, accessibility, and human connection shape people's experiences in an increasingly digital world. Her academic interests have led her to explore artificial intelligence, persuasion, social media, and data privacy through university summer programs and independent research. Her research on why people comply with scam requests despite their doubts, and how AI may make those requests more persuasive, reflects her interest in understanding the social and psychological forces behind the choices people make.

References

Chanenson, J., Matthews, T., Consolvo, S., Kelley, P. G., McClearn, J., Meiklejohn, S., Roy, A., Shelby, R., Thomas, K., & Hassoun, A. (2026). "It didn't feel right but I needed a job so desperately": Understanding people's emotions and help needs during scams. In Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (pp. 1-22). ACM. Author-posted version consulted. https://doi.org/10.1145/3772318.3790556 Full text: https://arxiv.org/pdf/2604.06218

Czybik, S., Kouam, A. J., Heubl, P., Nold, J. M., & Rieck, K. (2026). A large-scale study of personalized phishing using large language models. In Proceedings of the 35th USENIX Security Symposium (pp. 1687-1706). USENIX Association. https://www.usenix.org/conference/usenixsecurity26/presentation/czybik Full text: https://www.usenix.org/system/files/usenixsecurity26-czybik.pdf

DeLiema, M., Fletcher, E., Kieffer, C. N., Mottola, G. R., Pessanha, R., & Trumpower, M. (2019, September). Exposed to scams: What separates victims from non-victims? FINRA Investor Education Foundation, BBB Institute for Marketplace Trust, and Stanford Center on Longevity. https://www.finrafoundation.org/sites/finrafoundation/files/exposed-to-scams-what-separates-victims-from-non-victims_0_0.pdf

DeLiema, M., Li, Y., Taylor, M. K., & Mottola, G. R. (2022, November). Does one size fit all? An examination of risk factors by scam type. FINRA Investor Education Foundation. https://www.finrafoundation.org/sites/finrafoundation/files/2024-10/Does-One-Size-Fit-All-An-Examination-of-Risk-Factors-by-Scam-Type-Brief.pdf

Europol. (2025). Steal, deal and repeat: How cybercriminals trade and exploit your data. Internet Organised Crime Threat Assessment 2025. https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

Federal Bureau of Investigation. (2024, December 3). Criminals use generative artificial intelligence to facilitate financial fraud. Internet Crime Complaint Center, Public Service Announcement I-120324-PSA. https://www.ic3.gov/PSA/2024/PSA241203

Federal Trade Commission. (2023, July). How to avoid a scam. Consumer Advice. https://consumer.ftc.gov/articles/how-avoid-scam

Federal Trade Commission. (2025a, June). How to spot, avoid, and report fake check scams. Consumer Advice. https://consumer.ftc.gov/articles/how-spot-avoid-and-report-fake-check-scams

Federal Trade Commission. (2025b, December 1). Protecting older consumers 2024-2025: A report of the Federal Trade Commission. https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf

Federal Trade Commission. (2026a, March 25). The rising scam economy: Modernizing federal approaches to protect Americans from foreign fraudsters. Prepared statement before the United States Congress Joint Economic Committee. https://www.ftc.gov/system/files/ftc_gov/pdf/ftc-testimony-jec-hearing-on-the-rising-scam-economy.pdf

Federal Trade Commission. (2026b, June). What to do if you were scammed. Consumer Advice. https://consumer.ftc.gov/articles/what-do-if-you-were-scammed

Fontes, A., Valdes, O., Mottola, G., Ganem, R., & Green, S. (2026, March). Confident you can detect financial fraud? Think again. FINRA Investor Education Foundation, Consumer Insights: Money & Investing. https://www.finrafoundation.org/sites/finrafoundation/files/2026-03/Consumer_Insights_Brief_Confident_You_Can_Detect_Fraud_Think_Again.pdf

Honick, C., DeLiema, M., Fletcher, E., Mottola, G. R., Pessanha, R., & Trumpower, M. (2021, September). Exposed to scams: Can challenging consumers' beliefs protect them from fraud? FINRA Investor Education Foundation, BBB Institute for Marketplace Trust, and University of Minnesota. https://www.finrafoundation.org/sites/finrafoundation/files/exposed-to-scams-can-challenging-consumers-beliefs-protect-them-from-fraud.pdf

Kircanski, K., Notthoff, N., DeLiema, M., Samanez-Larkin, G. R., Shadel, D., Mottola, G., Carstensen, L. L., & Gotlib, I. H. (2018). Emotional arousal may increase susceptibility to fraud in older and younger adults. Psychology and Aging, 33(2), 325-337. https://doi.org/10.1037/pag0000228 Full text: https://web.stanford.edu/group/mood/cgi-bin/wordpress/wp-content/uploads/2018/10/Kircanski_gotlib_fraud_2018.pdf

Scams Against Older Adults Advisory Group. (2024, April). A review of scam prevention messaging research: Takeaways and recommendations [Report of the Scam Prevention Research Committee]. Federal Trade Commission. https://consumer.ftc.gov/system/files/consumer_ftc_gov/pdf/A%20Review%20of%20Scam%20Prevention%20Messaging%20Research.pdf

Scheibe, S., Notthoff, N., Menkin, J., Ross, L., Shadel, D., Deevy, M., & Carstensen, L. L. (2014). Forewarning reduces fraud susceptibility in vulnerable consumers. Basic and Applied Social Psychology, 36(3), 272-279. https://doi.org/10.1080/01973533.2014.903844

Appendix A: Sources and research notes

Personal accounts

Debby's account is shared with permission. My experiences with Tech Talk for Seniors and summer courses provide the personal context for this inquiry. These experiences were not collected as a formal interview study. Jackie and Karl are pseudonyms used in the published research.

Published evidence

The review used original government publications, reports written by the researchers, and academic papers. I selected sources relevant to the paper's questions rather than conducting a comprehensive search of research databases. The 2019 and 2022 DeLiema reports appear to draw on the same underlying survey and should not be treated as separate studies confirming the same findings. The 2021 interview report belongs to the same broader research program. For the Chanenson paper, I consulted the version posted by its authors. Its researchers rephrased quoted posts for privacy. The present paper paraphrases their account rather than quoting original Reddit wording.

The March 2026 FTC testimony provides overall fraud-report and reported-loss figures for 2025; the December 2025 older-consumer report provides age comparisons for 2024. The latter excludes data from the FBI's Internet Crime Complaint Center (IC3) from its age analysis because of differences in the age ranges collected. This paper does not combine FTC and FBI totals or treat those figures as estimates of losses caused by AI. Page citations to reports refer to printed page numbers; section citations identify the relevant academic-paper discussion.

Appendix B: Claim and source map

This map identifies the principal evidence claims. The three-condition interpretation and proposed responses are distinguished from measured findings in the main text.

Claim or measure	Source and location	Interpretive boundary
2025 reported fraud totals	FTC, 2026a, p. 2	Dated reporting snapshot; no AI attribution or exposure denominator.
2024 age comparisons	FTC, 2025b, pp. 18, 21-22	Reporting and median-loss measures; incomplete age coverage.
Confidence and hypothetical investment	Fontes et al., 2026, pp. 3-4, 8	Survey intentions; no actual investment or inferred individual overlap.
Associations by scam type	DeLiema et al., 2022, pp. 1, 3-5	Selected reporters; response and loss differ; no causal trait ranking.
Doubt alongside felt obligation	Chanenson et al., 2026, sections 3.3, 3.5, 4.1.2, 4.3.1	Qualitative interpretation of selected self-reports.

Claim or measure	Source and location	Interpretive boundary
Arousal and purchase intention	Kircanski et al., 2018, pp. 329-334	Primary responder analysis; no actual fraud-loss outcome.
Discussion during an encounter	DeLiema et al., 2019, pp. 2, 12	Association among those who engaged; no intervention effect.
Jackie and Karl	Honick et al., 2021, pp. 1, 14, 17-18	Pseudonymous reported experiences.
Personalized phishing	Czybik et al., 2026, sections 5-6, 8.2	Institutional click outcome; no general financial-loss multiplier.
AI misuse and stolen data	FBI, 2024; Europol, 2025, pp. 4, 6, 11, 14	Official threat descriptions; cumulative breach effect unquantified.
Changing help needs	Chanenson et al., 2026, section 4.2	Stage distinctions; proposed responses require testing.
Checking and recovery guidance	FTC, 2023, 2025a, 2026b; FBI, 2024	Existing guidance; proposed wording untested; recovery not guaranteed.
Open research question and precedent	Scams Against Older Adults Advisory Group, 2024, pp. 2, 10; Scheibe et al., 2014	Committee review; does not necessarily reflect members' views; staged calls with prior victims, no payment requested; same-scam warning effect not detected at four weeks.