IOSR Journal of Economics and Finance (IOSR-JEF)
e-ISSN: 2321-5933, p-ISSN: 2321-5925, Volume 16, Issue 4 Ser.1 (Jul. – Aug. 2025), PP 08-12
www.iosrjournals.org

The Role of Behavioural Economics in Understanding and Countering Fraudulent Tactics

AUTHOR

Agboola, Olatoye Kabiru
Department of Business Analytics & Data Science,
School of Business, New Jersey City University,
Jersey City, New Jersey, USA.
ORCID iD: 0009-0004-0905-0175
agboolaolatoye@gmail.com

Abstract
Around the world, schemes such as psycho-phishing and investment frauds cause huge economic and social problems. In the U.S., people lost more than $10 billion to fraud in 2023. These schemes rely on the usual ways people make decisions. Within behavioural economics, researchers are finding out how fraudsters abuse common shortcuts and feelings and how guidance and policies can help people become more resistant to fraud. This article looks closely at this area of research, stressing examples from all over the globe as well as from Nigeria. The paper discussed how behavioural economics sheds light on both why victims fall for scams and what tactics scammers use and how it can lead to helpful steps such as public awareness campaigns and redesigning the way choices are laid out to combat fraud.

Date of Submission: 23-06-2025 Date of Acceptance: 04-07-2025

I. Behavioural Economics: Foundations

Behavioural economics differs from classic models because it includes psychological factors when making economic choices. It understands that people make uncertain choices using mental shortcuts and are sometimes affected by specific mistakes in thinking. Classic research from Kahneman and Tversky finds that the judgment of probabilities is affected by what can be recalled from recent experiences (availability bias) and similarity to things known (representativeness bias). People feel losses more strongly than gains and tend to measure their decisions in relation to their own frames of reference (Prospect Theory). The process of thinking is frequently categorized as fast and intuitive (System 1) or slow and deliberate (System 2). Because these patterns exist, real choices are generally different from those of a completely logical agent.

It is commonly known that people prefer to see themselves in good light. It is predicted in these models that people will be dishonest only as far as it helps them feel good about who they are. As Mazar, Amir and Ariely (2008) also discovered, people are willing to cheat slightly to earn extra money, but they draw the line after that to prevent feeling guilty. In practice, individuals usually decide to make less money in order to minimize psychological regret from dishonesty. Moreover, asking people to sign honesty pledges ("sign here if you promise to tell the truth") has been proven to increase honesty. In one laboratory and field study, those who signed an honesty declaration before providing their results cheated a lot less than those who signed afterwards. Just asking customers to sign at the beginning of a document helped them think about ethics at the right time and it reduced the chances of dishonest actions.

An important part of behavioural economics is focusing on nudging (Thaler & Sunstein, 2008) which means making small adjustments to the environment to help channel decisions in favorable ways without eliminating different options. Using the phrase "about 90% of others in your profession handle it promptly" (a social norm nudge) tends to make more taxpayers follow the rules. When people are given both clear advice and social norms, it has led to big improvements. According to the UK Behavioural Insights Team, simple changes in tax forms such as including bold keywords and social honesty messages ("97% of healthcare workers file tax correctly"), made more people answer them. Send a letter telling patients that almost all of their colleagues comply, along with a warning about the risk of fraud and this approach is much more effective. What this

suggests is that changes in social attitudes, how obvious problems are and simplicity may encourage people to act properly and discourage misconduct.

In short, behavioural economics records various regular choice mistakes (such as present bias or being overconfident) that fraudsters can benefit from. It also proposes special ways to intervene (e.g. reminders, norm-based messages, redesigning paperwork) to help manage these biases. After that, how fraud happens and who it affects are looked at.

II. How Fraudsters Exploit Behavioural Biases

It is typical that fraudsters plan their scams around known persuasion and cognitive biases. Social psychologists have found that there are certain persuasion principles (Cialdini's six: reciprocity, authority, social proof, liking, consistency, scarcity) that guide people's choices. Many studies show that scammers often depend on the same principles as these. Many phishing and advance-fee scams start by claiming to be from an authority ("I am a prince/concert promoter/official") and appeal to group pressure ("your friends have already put money into this"). Other attacks give the victims a sense of obligation ("I gave you this chance, so now you must help me") or suggest that their decision must be made fast ("The deadline is tomorrow, make a choice now"). Ferreira and colleagues (2015) examined phishing emails and discovered that nearly every form of persuasion tactic is included, often used together in fraud schemes. All in all, people are often scammed because scammers "promote" a fake offer the same way merchants sell products.

A good example of this type of scam is the "Nigerian Prince" scam (advance-fee fraud). An email here poses as a high-ranking official, saying they are unable to leave a large sum of money in the country and that the helper can keep a portion of the money. The victim is told their money is unsafe, but they are asked to pay an initial "processing fee" before it can be recovered. The windfall is divided into small portions to build trust, while the story makes everything seem urgent and confidential (limited time to take action and risk discovered). As explained by Neuhaus (2020), scammers usually approach people this way: "I ask for help and I promise a generous commission to the victim." Let's not speak about this to anyone for now. People who fall victim to this get lured by the idea of quick earnings and do not consider the risks. A lot of these scams (such as pretending someone is kidnapped or you have a big lottery prize) depend on fear and fast feelings to convince people.

They also take advantage of when people are too confident or overly optimistic. A lot of scam victims feel they are financially smart which fools them into trusting others easily. Surveys point out that individuals who have little financial knowledge, but are very certain about it, are often easier to fool by fraudulent investment offers. In this study, individuals who feel especially good about their abilities were more likely to believe "get rich quick" pitches. Con artists often use the promise of great profits (encouraged by greed and optimism) and unsuspecting victims trust them. As shown by Xiao et al. (2022) in their study on Chinese individuals, both men and those with more education trusted their financial skills more, making them overconfident and this group of overconfident individuals expected to make abnormally large returns by investing. This makes it clear that flaunting positive outcomes might lead the overconfident to commit fraud.

Some other cognitive biases are also involved. Depending on if you present a risky deal as a potential loss or gain, people will react differently. Certain scammers threaten victims with tax debt or fines ("Pay me to stop you from getting into trouble with the government") and use this to get money. People often overestimate the effect they have on random events which might trick them into joining Ponzi schemes and think they can identify a winning investment. Confirmation bias means some victims will only focus on positive hints ("I got a response to my letter!"), while overlooking any negative signs.

Usually, fraudsters make sure their plots go unnoticed by most people. Using emotion in their stories, they hold the victims in a quick mode (System 1) in which people trust their instincts and take shortcuts. When issues with delays or higher costs come up, doubts about the investment start to rise, though perhaps it is already too late. Therefore, when someone reflects and thinks carefully before making a decision (System 2), they are less likely to fall for a scam, so scammers try to stop this reflection in their targets.

III. Psychological Tactics: Persuasion and Deception

Scammers build on heuristics by trying to make victims believe and obey them, using social engineering. Phishing campaigns often pretend to be an important letter from a recognized source to take advantage of that trust. Criminals may build virtual friendships with their targets to make them easier to manipulate (people often do what their friends ask). These romantic scams are clear examples: crooks set up attractive online profiles, await trust and build their victims' confidence over time. People who fall for romance scams are often seen to have a high level of trust and quick decision-making. According to Whitty and Buchanan (2018), people who become victims of online dating scams rated higher in both trusting behaviors and sensation-seeking. Fraudsters use these traits by telling stories that arouse concern and sympathy (e.g. about someone traveling who is in trouble and needs help). People who get scammed usually say they felt as abandoned as if a loved one had left them, even with prior doubts.

Fraudsters depend on creating a need for speed and jeopardy. A lot of fake emails state that the opening is limited and only you are aware of it ("contact me only within 24 hours about this job!"). This creates pressure by ensuring there is not enough to waste time deciding. Some investment scams might claim that a lot of people are already taking part in the investment to make the offer look more appealing. A scammer may start by asking you for only a slight act of trust (intro or small contribution) and progress to larger commitments over time (foot-in-the-door effect). Whenever the victim says yes, it becomes less likely that they will withdraw from the situation later.

At the end, many criminals try to sway the victim's image of themselves. There are scripts that try to make someone seem important by complimenting them (saying you're one of the smartest) and there are scripts that create fear by pretending to be debt collectors. You can always see behavioural strategies being used. Basically, fraud is a type of "brain hacking", where threats are molded to trigger specific and expected responses from humans.

IV. **Victim Vulnerabilities: Who Falls Prey?**

Being familiar with fraud includes identifying the most at-risk groups. There is a significant effect of behaviour in addition to demographics. Many studies have looked into how victims think and feel. Lack of knowledge about technology and help from others makes the elderly easy for cybercriminals to target. A study by DeLiema et al. (2024) on 20 years of mail-scam incidents discovered that seniors older than 70 are more often victims of repeated scams than people in their 40s to 60s. Those in their early 60s to late 70s were much more likely to experience multiple scams than adults aged 50-59. Young adults (between 18 and 29) saw fewer cases of repeat scams. Age makes people more likely to lose more when they are scammed, as cognitive problems, feeling lonely and being less aware all increase their risk. Actually, studies report that people who feel isolated are at risk: they often feel lonely or depressed, so scammers take advantage of their situation. Some police investigations found that lonely people were picked by perpetrators who built friendships and, from these, manipulated the victims. So, mental condition and society play a role that is as great as age itself.

There is a relationship between gender, education and the way people act. They also investigated romance scams and discovered that common characteristics among victims were being middle-aged, highly educated and having high impulsivity and trust levels. Such characteristics (lacking control of urges, trusting people too easily) helped scammers because they made victims more willing and gullible. Studies usually find that people who do not understand finances well and are overconfident, are more likely to commit fraud. According to Cucinelli and Soana (2023), people with average financial knowledge but who believe they know more are more likely to be victims of investment fraud. Academics point out that investors with little knowledge are more likely to miss fraud and self-assured investors are less cautious about possible losses. Xiao et al. (2022) also found that people who are overconfident are more likely to accept the idea of unusually high returns. Rather, people who take time to review offers before accepting them are more protected against scams.

Behavioural biases play a part everywhere: factors such as how tolerant a person is to risk, their curiosity for sensations and whether they trust someone can change the outcome. Based on their study, Bensinger et al. (2019) discovered that people who fall for scams have greater belief in others and like more exciting activities. Then again, having strong reasoning and being critical offers protection. Sadly, a lot of individuals think they are immune to the risks – this is a well-known bias known as optimism. Because of this, victims may overlook signals like being asked for money by strangers.

Nigeria stands out in having these issues. Because Nigeria is rushing headlong into digitalization, there are more chances for fraud at home and abroad. People and businesses in Nigeria have experienced huge phishing and SIM swap attempts. Lately, a study showed that following COVID-19, 42% of people using digital financial products in Nigeria encountered phishing attempts. A lot of Nigerians are wary of using digital payment systems as well. How people behave also plays a part: not knowing much about online safety and putting a lot of trust in friends can result in missing red-flags like phishing websites. In Nigeria, same tricks are used: media reports called "Yahoo Boys" mention that they use fake social media and investment strategies to lure people, just as in Western countries. For this reason, Nigeria becomes a target and also takes part in the worldwide scam stories.

V. **Countering Fraud through Behavioural Interventions**

If fraud comes from behavioural biases, then addressing those behaviors can fight fraud. Two forms of strategies are introduced by the literature: "pre-emptive nudges" and broader approaches.

- **Educating and informing people.** Helping people see and understand popular strategies and biases can be direct. A lot of governments and NGOs launch campaigns to teach people how to stop and make sure a request is genuine. For example, workshops and information programs on the radio are used in Nigeria to alert people about frequent scams. Even so, noticing the problem does not always fix it. Byrne et al. (2024) discovered in their Nigerian study that having an educational program for small business owners increased trust

in digital payments and general understanding of fraud, but participation did not boost their ability to spot real scams. People considered themselves less likely to fall for scams, yet their results on a test of actual and fake emails didn't change. In fact, being trained made people more certain in their (unchanged) skill to spot fraud. The result makes it clear that simply providing information may not alter the common ways of thinking.

- **Nudges and choice architecture**. It gives public administrators new approaches to change things. Modifying how forms and messages are designed may prevent people from being dishonest. You could use the simple "sign-at-beginning" method elsewhere such as on online forms to ensure users are honest early on. Encouraging people by saying "it's normal to use 2FA" or "most users ignore suspicious emails" is another way. Emphasizing that "97% of people just like you file their taxes on time" made filing more likely for the majority of people. The same idea could be helpful when fighting fraud: an example would be a pop-up after every banking login that says, "More than 95% of Nigerians double-check their transfers before sending money." This may lead people to take a moment and think before they approve a scam transaction.
- **Guardrails in digital systems**. Many designers who work on platforms use behavioural design for security. If a suspicious email is found, for example, many email apps now slow things down or place markers to warn users. These cues make users pause and think about what action to take (shifting from instinctive to careful thought). Chou et al. (2021) found that some people become victims of phishing because alluring or pressuring elements in the messages make them act impulsively. Interventions such as flashing texts ("This email could be unsafe!") might make people think twice about their actions. A type of nudge called browser alert which reminds you of problems linked to password reuse or unsafe downloads and leads many users to take security precautions. Behavioural remedies should be judged with care: According to Byrne et al., simply giving repeated examples in Nigeria did not achieve better detection, demonstrating that messages should be engaging.
- **Organizational culture and ethics**. Using behavioural insights, companies help prevent internal fraud. To illustrate, some companies ask employees to sign an integrity pledge at the start or publicly agree to ethical standards (taking advantage of consistency bias). It is possible to view auditing processes as widely used (people see that things are being checked). One technique employed in governments is to let employees find out via small announcements that transparent actions are the standard among their peers; this can hugely increase reports of dishonest acts. Studying within Slovakia, field experiments that showed workers examples of responsible leaders found a huge increase in the chance workers reported potential risks of fraud. While this work happened in Europe, its lessons have close connections with ethics in any culture. If stories about honest officials are publicized in Nigerian civil services, it could influence others to be more honest as well.
- **Legal and structural reforms**. In the end, behavioral strategies need to be used alongside strengthening the framework. tired institutions as well as personal biases give an advantage to fraudsters. Pressure for money, no effective controls and moral excuse are the factors behind fraud that behavioural economics stresses are part of the "fraud triangle," beyond just looking at choices. Relative legality can be reduced by ensuring tough verification, better oversight and encouraging new principles (such as anti-corruption pledges). Anti-corruption experts in Nigeria argue that the presence of group norms strongly supports bribery and fraud. Projects of this kind, like SNAG, want to move social habits by telling us that most citizens still oppose corruption, even while thinking that everyone does it. Studies indicate that emphasizing that fraud is wrong can deter people from thinking it is normal and diminish their willingness to engage in fraud.

All things considered, some behavioural choices do not always work. Academics are not sure which nudges apply to most situations. In other fields, most interventions designed by nudge theory have either not worked when researched again or had little success. Byrne et al. Nigeria fraud trial serves as a good lesson for everyone. It implies that briefly trained employees or just a few emails might not work well – mainly if large sums are on the line and malicious actors can shift tactics fast. This underscores that combating fraud requires a multi-layered approach: **technology, education, policy and design** must reinforce one another.

Behavioral Economics: A Global and Nigerian Perspective

While fraud exists worldwide, the culture and institutions of each place affects how people act to commit it. Trust norms vary from one society to another which means persuasion is not the same everywhere. Advance-fee "419" scams which started in Nigeria, have caused problems for Western targets overseas. Criminals transfer frequently used tricks (greedy urges) to trick people around the world. However, Nigerians are victims of special local scams, including romance on WhatsApp, false lottery promises and online fraud using official-sounding notes in the common local languages. In Nigeria, recent studies (for instance, those by Trinity and IPA) have attempted to capture these hidden trends.

It is clear that digital trust-building is very important in Nigeria. The trial recorded that being part of the training course boosted users' confidence in digital payments and made them more willing to use them. This means that a lot of Nigerian small businesses want to embrace digital finance, but they often hesitate because of scam concerns. Some warnings against fraud highlight being cautious so frequently that they end up reducing people's trust even more. Alternatively, giving fraud warnings should be mixed with words of encouragement

(for example, 'most transactions can be trusted') and possible means of protection (such as letting users adjust their limits or set reminders). Mobile money in Nigeria could initially set small spending limits for all users, unless they answer questions about common frauds.

Public procurement and people being involved in corruption is another important issue in Nigeria. The Economic and Financial Crimes Commission (EFCC) in Nigeria finds that public offices are affected by widespread fraud. Experts say officials' reasoning for embezzling can be like how people justify giving a bribe. Suggestions have been made to motivate people to act more honestly in government. Chatham House points out that the majority of Nigerians consider corruption (an example of systemic fraud) to be the biggest issue with governance. They mention "role models" and "integrity networks" – that is, building on social influence and shared knowledge to change behaviors. Much like showing staff good ethical examples has encouraged others to blow the whistle, introducing anti-fraud cases through mentoring programs can form better social standards among civil servants.

All in all, behavioural economics provides both a way to understand and also the means to carry out fraud. It describes who con artists pick and how they dream up their schemes. It also proposes specific solutions to help: advertising the importance of honesty, encouraging trust through social standards and changing the environment for decisions to make them slower. Both places, Silicon Valley and Lagos, are affected by the same main biases. Though case studies from Nigeria show that interventions must adapt to each region's culture and trust, the basic behavioural rules do not change.

VI. **Conclusion**

Methods used in fraud work by manipulating common parts of human psychology. Many become victims of scams because of easy thinking habits, reactions to emotions and social conditions. Behavioural economics explains all this by pointing out important shortcuts that can tip behavior: overconfidence, scarcity bias, social proof and more. It lays out approaches for protective action too which take into account human understanding in real cases. It has been determined that using behavioural insights can greatly improve anti-fraud approaches on a global scale as well as in Nigeria.

Even so, research cautions that behavioural approaches are not the ultimate answers. A lot of nudges have brought about mixed outcomes when used in fraud prevention. Being overconfident and thinking the same way all the time can stop us from accepting simple messages. So policymakers and practitioners ought to use both behavioral steps and advanced controls and technology in their processes. When anomalous transactions are detected by machine learning algorithms, the users should be notified clearly and believably through a user interface.

Finishing the research means taking it a step further. To advance further, "fraud economics" should try interventions in several scenarios and across cultures. Nigeria which is both involved in committing fraud and suffering from it, makes it a great subject for these studies. Meanwhile, realizing vulnerabilities, using helpful reminders and improving the system gives us the best chance to stop fraudsters from cheating innocent people.

References

[1]. Amir, O., Mazar, N. and Ariely, D., 2008. The dishonesty of honest people: A theory of self-concept maintenance. *Journal of Marketing Research*, 45(6), pp.633–644.

[2]. Byrne, S., Putman, D., King, M. and Jang, C., 2024. Navigating the rise in non-institutional digital fraud: An experiment with micro enterprises in Nigeria. *Trinity Economics Papers*, No. 1224. Trinity College Dublin.

[3]. Chatham House, 2025. *Taking action against corruption in Nigeria: Empathy, entrepreneurship and new approaches*. Chatham House Research Briefing.

[4]. Cialdini, R.B., 2009. *Influence: Science and practice*. 5th ed. Pearson.

[5]. Cucinelli, D. and Soana, M.-G., 2023. Are financially illiterate individuals all the same? *International Journal of Bank Marketing*. Advance online publication. https://doi.org/ (insert DOI if known).

[6]. DeLiema, M., 2020. Financial fraud among older Americans: Evidence and implications. *The Gerontologist*, 60(Suppl_1), pp.S6–S15.

[7]. DeLiema, M., Langton, L., Brannock, D. and Preble, E., 2024. Fraud victimization across the lifespan: Evidence on repeat victimization using perpetrator data. *Journal of Elder Abuse & Neglect*, pp.1–15.

[8]. Ferreira, A., Coventry, L. and Lenzini, G., 2015. Principles of persuasion in social engineering and their use in phishing. In: *Lecture Notes in Computer Science*, Vol. 9190, pp.127–142. Springer.

[9]. Lichtenberg, P.A., Stickney, L. and Paulson, D., 2013. Is cognitive functioning related to perceptions of fraud risk in older adults? *Journal of Elder Abuse & Neglect*, 25(3), pp.211–225.

[10]. Lichtenberg, P.A., Sugarman, R.L., Paulson, D., Ficker, L.J. and Rahman-Filipiak, A., 2016. Loneliness, loss, and the challenge of sustaining fraud prevention in a cashless economy. *Journal of Elder Abuse & Neglect*, 28(4–5), pp.293–309.

[11]. Mazar, N., Amir, O. and Ariely, D., 2008. The dishonesty of honest people: A theory of self-concept maintenance. *Journal of Marketing Research*, 45(6), pp.633–644.

[12]. Neuhaus, T., 2020. A nudge-psychology reading of the "Nigerian scam". *Brolly – Journal of Social Sciences*, 3(3), pp.7–28.

[13]. OECD, 2017. *Behavioural economics and financial consumer protection*. OECD Publishing.

[14]. Shu, L.L., Mazar, N., Gino, F., Ariely, D. and Bazerman, M.H., 2012. Signing at the beginning makes ethics salient and decreases dishonest self-reports in comparison to signing at the end. *Proceedings of the National Academy of Sciences*, 109(38), pp.15197–15200.

[15]. Whitty, M.T. and Buchanan, T., 2018. "Do you love me?": Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior, and Social Networking*, 21(1), pp.3–8.
[16]. Whitty, M.T. and Buchanan, T., 2015. The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law*, 21(3), pp.209–223.
[17]. Byrne, S., Putman, D., King, M. and Jang, C., 2024. Navigating the rise in non-institutional digital fraud: An experiment with micro enterprises in Nigeria. *Trinity Economics Papers*, No. 1224. Trinity College Dublin.
[18]. Federal Trade Commission, 2024. As nationwide fraud losses top $10 billion in 2023, FTC steps up efforts to protect the public [Press release]. 9 February. Available at: https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public [Accessed 18 Jun. 2025].
[19]. Finance Times, 2012. Why so much fraud in academia? Available at: https://freakonomics.com/podcast [Accessed 18 Jun. 2025].
[20]. Kahneman, D., 2011. *Thinking, fast and slow*. Farrar, Straus and Giroux.
[21]. Thaler, R.H. and Sunstein, C.R., 2008. *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press.