Using Behavioural Economics to Understand and Prevent Authorised Push Payments Fraud

October 2025

Axiom Economics

Contents

This report was prepared for the Payment Systems Regulator by Axiom Economics Ltd, London, United Kingdom.

https://axiom-economics.co.uk/

https://www.linkedin.com/company/axiom-economics/

1. Executive Summary

This report explores how behavioural economics can shed light on consumer vulnerability to Authorised Push Payment (APP) fraud, and how it can inform the design of further interventions to prevent this type of fraud.

APP fraud is a deceptive crime where individuals are manipulated into transferring funds to criminals. Fraudsters exploit the behavioural biases of their victims, and behavioural economics has developed a rich typology of such biases. This typology has been applied across financial services and wider public policy to understand consumer behaviour in many contexts. Here, it is applied to understanding susceptibility to APP fraud.

In the context of APP fraud, the four primary biases which may make consumers susceptible are: i) vulnerability to scarcity; ii) willingness to trust; iii) susceptibility to interpreting the illusory as true (the representativeness heuristic); and, iv) susceptibility to being rushed and pressured into fast choice (System 1 vs System 2 thinking). For example, in purchase scams, fraudsters present products at prices that are "too good to be true" (exploiting vulnerability to scarcity); purporting to be a known and trusted brand mimicking the look and feel of legitimate transactions (willingness to trust); with product descriptions that often include recognised and premium details to make the offer seem genuine (the representativeness heuristic); and create urgency by framing the deal as a short-term opportunity that needs immediate payment (System 1 thinking).

Within each of these headline behavioural biases, fraudsters exploit a series of secondary biases, such as making a too-good-to-be-true deal eye-catching to allure consumers who are vulnerable to scarcity.

Behavioural economics offers insights into the design of interventions to reduce the occurrence of APP fraud. Interventions targeted at customers should ideally deter them from making transactions which are at high risk of being fraudulent. To do so while preserving individual choice, such interventions should prompt the consumer to re-evaluate the prospect and consider whether it is indeed “too good to be true” (e.g. the purchase, romance, or apparent emergency message from the tax authority) and slow down the transaction to allow deliberation and delay to payment.

However, there needs to be an economic balance between the benefits of interventions designed to slow payments and the benefits of offering a fast and efficient payments system. While there are economic and societal costs to APP fraud which are borne privately (by the victims) and socially (by the wider social costs of fraud), there are also likely to be economic and societal costs associated with slowing or stopping legitimate payments. Behavioural remedies should therefore where possible seek to reduce “illegitimate” payments which are associated with fraud, while maintaining or increasing the completion of “legitimate” payments.

In the UK, and noting that regulatory action has already been taken by the Payment Systems Regulator (PSR), behavioural economics suggests that there could be benefits of *targeting* and *repositioning* risk warnings as part of further developing steps to address APP fraud. Lack of targeting could cause two inefficiencies. First, it potentially risks slowing or deterring legitimate payments and could create costs in the payment system, compared to if there were more risk-based targeting. Second, it potentially renders warnings less effective by creating cognitive fatigue and muscle memory effects. These have been demonstrated in a number of choice domains, and could also be present in customer payments journeys, reducing the efficacy of interventions. A more effective deployment could see risk warnings targeted to higher-risk transactions, defined by transaction characteristics, with salient calls to action. Positioning is also crucial, such as whether the risk warning is positioned in the purchase journey or the transaction journey.

Taking into account the literature and toolkit of behavioural economics, and applying it to APP fraud, our analysis suggests that the effectiveness of risk warnings could vary depending on factors such as, i) at what stage they are delivered, for instance, during the purchase or at the payment stage. The purchase stage typically exists on an online platform or marketplace separate from the payment journey; ii) the extent to which risk-based approaches are taken to targeting transactions deemed high risk and concurrently removed from transactions deemed low risk. A less-is-more approach to risk warnings could overcome muscle memory and cognitive fatigue effects which can dull the effectiveness of warnings, and iii) there could be benefits to understanding and tailoring approaches to heterogeneity in susceptibility and exposure across the payments population, targeting those who are both susceptible and more likely to be exposed to APP fraud.

2. Introduction

Authorised Push Payment (APP) fraud, a deceptive crime where individuals are manipulated into transferring funds to criminals, has become a commonplace form of consumer fraud over the past decade. APP fraud manifests in a variety of forms including purchase scams, romance scams, and impersonation scams. In each case, fraudsters engage in deception, such as offering a laptop for sale, posing as a romantic interest subsequently claiming to be in financial need, or the impersonation of a senior colleague at work with an emergency spending need, all aimed at extracting payment from their victim. The scale of APP fraud is significant, with around £0.5bn stolen from the more than 180k consumers who fall victim to APP fraud each year (UK Finance, 2025). APP fraud represents a significant cost to payment service providers who, following action by the PSR, are obliged to reimburse consumers for their losses from October 2024. This form of fraud also inflicts significant psychological and emotional costs on consumers and may contribute to reducing trust in payments and financial services.

This report aims to provide an expert-level analysis of how behavioural, psychological, and economic forces interact to influence consumer susceptibility to APP fraud. It explores the mechanisms of manipulation, the cognitive and emotional vulnerabilities of victims, and the individual and situational factors that increase risk. Furthermore, the report reviews potential prevention strategies, emphasising how behavioural insights can enhance their effectiveness. It does not seek to evaluate or provide a commentary on the PSR's recent regulatory action in relation to APP fraud (noting that the PSR is committed to an independently led evaluation of its rules) or broader steps by industry to address APP fraud. It is a review of the relevant insights from behavioural economics and their applicability to APP fraud.

Behavioural economics offers insight into both why consumers are deceived by APP fraud, and potential solutions which could reduce consumer susceptibility. Human behaviour and behavioural vulnerabilities are central to APP fraud because fraudsters exploit human vulnerability in their deception. Since victims themselves initiate the payment, albeit under false pretenses, in the domain of APP fraud the focus shifts from the exploitation of technical security vulnerabilities to the psychological manipulation that drives victims' decision-making. This fundamental

characteristic positions behavioural economics as an important lens for understanding and preventing this form of financial crime.

Fraudsters engaged in APP fraud exploit many of the biases and vulnerabilities in human behaviour which have been identified by behavioural economics in recent decades. Fraudsters exploit human vulnerability to scarcity, willingness to trust, tendency to over-interpret the illusory as true, and susceptibility to being rushed and pressured into making fast choices. Each of these behavioural biases is well known to behavioural economics, and also to those seeking to perpetrate fraud. Behavioural economics therefore provides a lens through which we can understand the techniques and tactics of fraudsters in exploiting human vulnerability. This report analyses these in detail and provides a typology of behavioural biases exploited by fraudsters.

Behavioural economics also offers, however, insight into the forms of intervention that might work against the tactics of fraudsters to reduce consumer victimisation. In a wide variety of domains, from food choices to energy usage, behaviourally informed interventions including nudges have been shown to be effective at improving consumer outcomes. We consider the same may be possible in the context of APP fraud, helping to further build on existing regulatory and industry action. The toolkit of behavioural economics is extensive, and there may be opportunities to push back against the exploitation of consumers' vulnerabilities by fraudsters.

This report highlights a number of factors that may impact the effectiveness of risk warnings. It builds on previous analyses undertaken by the Financial Conduct Authority (FCA), and we are grateful to the FCA for sharing an earlier-stage literature review. We are also grateful to the FCA and PSR for their input into earlier versions of this report.

3. Importance of behavioural economics in the context of payments fraud

Behavioural economics has emerged over the past 40 years as the study of human behaviour and the systematic errors and biases which affect individual decision-making. Behavioural economics presents a direct challenge to the neoclassical assumption of the rational economic agent, or *homo economicus*. The field began by systematically documenting how human decision-making is subject to cognitive biases, heuristics, and framing effects, leading to predictable deviations from optimal choices. These psychological insights have been applied to economic contexts, exploring concepts including limited self-control, fairness, and loss aversion to explain real-world market anomalies that traditional theory could not. By integrating empirical evidence from psychology into economic models, behavioural economics has established a new paradigm that provides a more descriptively accurate and psychologically realistic understanding of how people actually make financial and economic decisions.

Behavioural economics as a lens on consumer vulnerability

In traditional models of economic rationality, any mistakes in individual choices were considered random deviations from rational rules (Samuelson, 1947; Friedman, 1953; Arrow & Debreu, 1954). However, behavioural economics began with the documentation that these individual errors are not random but are instead systematic and relate to particular biases shared by individuals to a greater or lesser degree (Simon, 1955; Kahneman & Thaler, 1979; Thaler 1980).

The primary insight from behavioural economics is that human decision-making systematically deviates from what traditional economic models assume to be perfect, rational calculations. It reveals that our choices are shaped by a concept known as bounded rationality, which acknowledges that human cognitive abilities, information, and time are limited (for an introduction, see Simon, 1990). Consequently, people rely on mental shortcuts, or heuristics, to simplify complex decisions (e.g., Gathergood et al., 2019b; Gathergood et al., 2023). These heuristics can lead to predictable errors and cognitive biases. Key examples include loss aversion (see Schmidt & Zank, 2005), where the psychological pain of a loss is felt more intensely than the pleasure of an equivalent gain, and the framing effect (see, for example,

Tversky & Kahneman, 1974), where the way a choice is presented influences the outcome. Furthermore, behavioural economics demonstrates that decisions are heavily influenced by emotional and social factors, leading to behaviours like herd mentality and a preference for immediate gratification over long-term benefits. By integrating psychological realism, the field provides a more accurate understanding of why people make the economic choices they do.

The field has since developed a suite of theoretical models and empirical findings that support the idea that economic and financial choices are better understood when viewed through the lens of these biases. Consequently, policy-focused research has demonstrated how these biases can make consumers vulnerable to welfare losses, and in turn, how behavioural economics can inform policy design. Nevertheless, the discipline has faced scrutiny over the replicability of some results, the claimed magnitudes of effect sizes, and the sufficiency of its interventions for achieving desired outcomes (Beshears et al., 2024; Camerer et al., 2016; DellaVigna & Linos, 2022; Hume et al., 2024). In some cases, documented behavioural biases have not been replicated in other samples or contexts and behavioural “nudge” remedies have achieved only small impacts on desired outcomes. Studies have also documented unintended downstream consequences of behavioural nudges.

Application to financial and payments regulation

Behavioural economics has proven to be highly relevant to a range of areas of public policy through the concept of "nudging", which involves steering individuals towards better decisions without restricting their freedom of choice. Governments, most notably in the UK and the US, have established Behavioural Insights Teams to design and implement policies that account for predictable human biases. A prominent example is the dramatic increase in retirement savings through automatic enrolment in pension schemes, a policy that leverages the power of defaults and inertia to overcome procrastination (Thaler & Sunstein, 2008). Other applications include simplifying tax forms to increase compliance, using social norm messaging to encourage timely tax payments, and redesigning public communications to prompt healthier choices or increase organ donation rates, all of which have been suggested as successful implementations of nudging (Behavioural Insights Team, 2012). These interventions are designed to be low-cost and effective alternatives or complements

to traditional regulatory tools like mandates and bans, fundamentally changing how policymakers approach societal challenges.

Behavioural economics has become an important policy tool within financial regulation, in particular as it provides explanations for why some products can be welfare-reducing and may warrant being limited or even banned (see Dambe et al., 2013). In the UK, the widespread application of these insights was accelerated by the creation of dedicated bodies such as the Behavioural Insights Team in Cabinet Office and FCA Behavioural Economics and Data Unit, among others. For instance, the concept of impulsivity (where today's evaluation of the future in the impulsive state of mind is different from the evaluation that would be made tomorrow not in the impulsive state of mind), explains how consumers can make decisions that are not in their own long-term interests, leading to restrictions on financial products like payday loans (FCA, 2014) . Similarly, the default or status quo bias, where consumers stick with an existing option even when it is costly, prompted regulators to scrutinise auto-renewal practices that included "price walking" in the general insurance market (FCA, 2020). The distinction between "hot-state" System 1 thinking and "cool-state" System 2 thinking has also led to the introduction of mandatory cooling-off periods for finance contracts, allowing consumers to reconsider their choices (FCA, 2013).

As a consequence, research in behavioural economics has been used to develop a range of interventions in retail financial markets. In some cases, consumer vulnerability arising from behavioural biases has formed an evidence base for restricting or banning harmful products such as payday loans (e.g., Gathergood et al., 2019a), In other cases, behavioural interventions have been applied which seek to alter consumer choices. For example, information disclosures have been applied effectively to securities risk ratings and mandatory warnings for high-risk investments, addressing the fact that individuals do not always process readily available information by default (see FCA, 2021). Nudges have proven effective by leveraging the tendency for individuals to stick with defaults; this has been widely used in retirement saving design in the UK, which has also introduced automatic enrolment in workplace pensions (Cribb & Emmerson, 2016), as well as in environmental and food choice interventions. Finally, interventions designed to delay or slow down decision-making, such as "cooling-off" clauses, give consumers a

crucial opportunity to revisit their initial choices once they are in a more deliberative "cool" state and have been adopted across a variety of domains (see FCA, 2023).

Recent history of behavioural economics research in UK financial regulation

In the UK, behavioural economics research is actively used across the financial, insurance, banking, and payments sectors, all of which are closely connected to the issue of payment fraud. It has become a significant part of the toolkit for regulators because it offers the potential to develop high-impact policy interventions that often do not restrict consumer freedom of choice or require legislative changes. This approach allows for nuanced and effective regulation tailored to how people actually behave.

A substantial body of research has been developed by the FCA, which outlined its approach in its first Occasional Paper in 2013. Since then, the FCA has utilised a behavioural toolset in both its research and policy development. For example, it has tested the effectiveness of information disclosures through online trials, such as assessing the impact of supplementary investor factsheets on consumer understanding of funds (FCA, 2022). The regulator has also employed randomised trials of nudges, as seen in the Credit Card Market Study, which experimented with obscuring the option to make only minimum payments to see if it would reduce the number of customers in persistent debt (FCA, 2018). More recently, the FCA has used online experiments, including a simulated trading platform, to test the effects of "digital engagement practices" used by securities platforms, finding that they increase trading activity without improving investor outcomes (FCA, 2024). This research typically uses a combination of secondary data, surveys, and both online and real-world experiments to test hypotheses and simulate the potential effects of new policies.

Relevance to APP fraud

The insight into the existence of systematic biases in consumer behaviour is fundamentally important for research on APP fraud. Its relevance stems from the fact that behavioural biases are actively exploited by fraudsters, suggesting that interventions designed to overcome these biases could be a fruitful line of developing regulatory policy. Fraudsters commonly adopt the tactics of behavioural economics or science when attempting to defraud their victims. They employ specific

techniques designed to exploit cognitive vulnerabilities and may even target individuals identified as behaviourally vulnerable, on whom their methods likely will be most effective.

Studies often focus on interventions that might reduce consumer susceptibility to fraud in experimental settings. There is relatively less research on which types of vulnerability are most prevalent or whether these interventions work effectively in real-world settings. However, it is feasible to create simulated journeys that closely resemble real-world payment processes, allowing researchers to test hypotheses about consumer vulnerabilities and potential policy interventions, an approach used by Akesson et al (2023) to study fraud prevention.

Furthermore, interventions within payment journeys are typically low-cost (compared to other forms of intervention), as they are often designed and deployed digitally. This makes it potentially practical to roll out interventions widely. These digital interventions are also highly scalable and can be targeted to specific vulnerable groups based on their characteristics or through analysis of payments data.

4. Literature on biases relevant to APP fraud

This section presents a review of the existing literature on behavioural biases from the perspective of their relevance for understanding consumer vulnerability to APP fraud. Behavioural economics has revealed that human decision-making is subject to a wide array of systematic cognitive biases. This research has catalogued dozens of such biases, including well-known examples like loss aversion; the anchoring effect, where individuals rely heavily on the first piece of information they receive when making a decision; and the availability heuristic, where people overestimate the importance of information that is most easily recalled. While the full list of behavioural biases is extensive (for example, Stango & Zinman, 2023, examine 17 behavioural biases), demonstrating the complexity of human psychology, it also highlights a critical challenge for practical application: not all biases are equally relevant in every situation or to all individuals.

Therefore, for behavioural insights to be effective in a specific domain, such as preventing payment fraud or improving health outcomes, there is a crucial need to define the primary biases at play. Effective intervention requires empirical research to identify which specific vulnerabilities—be it impulsivity, overconfidence, or susceptibility to social pressure—are most potent and prevalent in that particular context, thereby allowing for targeted and impactful policy design.

Primary behavioural biases

Our review of the existing literature surfaces four primary behavioural biases as most relevant for understanding consumer susceptibility to APP fraud: vulnerability to scarcity, willingness to trust, the representativeness heuristics, System 1 / 2 thinking. Fraudsters adopt tactics in their design and implementation of APP fraud which exploit these biases, many of which are considered to be underlying long-running traits of human behaviour (Camerer & Loewenstein, 2006).

Vulnerability to scarcity. As explored in research by Shah et al. (2015), scarcity diminishes cognitive resources, causing individuals to focus intensely on their pressing, unmet needs. APP fraudsters weaponise this by creating offers or prospects that seem "too good to be true" but directly address a victim's specific scarcity. This can be economic, such as in purchase scams where an item is offered at a heavily discounted price to someone with limited resources available, or in

investment scams that promise unfeasibly high returns to those with insufficient savings. In each case, the state of scarcity (limited resources, insufficient savings) induces the victim to be more willing to believe the prospect is true. The principle also extends to non-economic dimensions, where emotional vulnerability or loneliness creates a form of social scarcity. This is a key feature of romance scams, where a fraudster feigns a deep connection to exploit the victim's need for companionship, ultimately leading to requests for financial assistance. In all these cases, the manufactured solution to a pressing need induces the victim to believe the fraudulent prospect is real, overriding their natural scepticism.

Willingness to trust. Another critical vulnerability is the willingness to trust, which fraudsters manipulate by appealing to authority or familiarity. As research has shown (e.g., Finn & Jakobsson, 2007; Judges et al., 2017; Luo et al., 2013), trust is a cognitive shortcut that can be powerfully exploited. In the context of APP fraud, perpetrators often achieve this by imitating entities that command a high degree of public confidence. For example, they might create sophisticated impersonation scams, posing as well-known retailers, a government body like HMRC, a utility company, or the victim's own bank. By using official-looking logos, email addresses, and language, they construct a veil of legitimacy. This tactic is also prevalent in business contexts through 'CEO fraud', where an employee is tricked into making an urgent payment by an email purporting to be from a senior executive, exploiting the inherent trust and authority within an organisation's hierarchy. The victim, believing they are interacting with a legitimate entity, is persuaded to authorise the payment.

Representativeness heuristic. The representativeness heuristic, first identified by Tversky & Kahneman (1974), is also fundamental to the success of many scams. This bias causes individuals to judge the plausibility of a situation by how closely it resembles a typical or representative example, rather than by its actual statistical probability. Fraudsters exploit this by ensuring their scams mimic the look and feel of legitimate transactions in almost every detail. For instance, a fraudster might advertise an implausibly cheap laptop on a fake website that is a perfect replica of a real one, complete with professional graphics, customer reviews, and a familiar checkout process. The victim's brain focuses on how much the scenario resembles a real online purchase, causing them to overlook the one detail that signals a fraud—the unrealistic price. As Chang & Chong (2010) note, this is closely related to

selective perception and the availability heuristic; the victim selectively focuses on the familiar, readily available cues of a genuine offer, making the scam appear credible despite its internal inconsistencies.

System 1/2 thinking. Finally, fraudsters actively try to manipulate victims into a state of System 1 thinking over the more deliberative System 2 thinking, a concept popularised by Kahneman (2011). System 1 is our fast, intuitive, and emotional mode of thought, while System 2 is slow, logical, and analytical. APP fraudsters engineer scenarios that create urgency, panic, or excitement to keep the victim firmly in a "hot state" of System 1 thinking. They might claim a bank account has been compromised and money must be moved immediately, or that a once-in-a-lifetime investment opportunity will vanish in minutes. By applying intense time-pressure and emotional manipulation, they prevent the victim from engaging System 2, which would otherwise logically assess the situation, question the inconsistencies, and identify the scam. This vulnerability may be amplified by individual characteristics such as impulsivity or limited self-control, making certain individuals more susceptible to falling for a fraudulent scenario when put under this type of cognitive load.

Secondary behavioural biases

The four primary behavioural biases at work in APP fraud can each be viewed as encompassing other sub-biases commonly held by individuals and exploited by fraudsters which can be categorized as in Table 1 below (though there is no consensus on this in the existing literature).

Table 1: Mapping Secondary Behavioural Biases			
Vulnerability to scarcity	**Willingness to trust**	**Representativeness heuristic**	**System 1/2 thinking**
Salience and perception (Chang & Chong, 2010)	Positive affect (Slovic et al., 2007)	Social proof (Roethke et al., 2020)	Hot/cool system (Metcalfe & Mischel, 1999)
Visceral influence (Langenderfer & Shimp, 2001)	Prestige bias (Dolan et al., 2012)	Availability effect (Braga et al., 2018)	Impulsivity (Ong, 2022)
Improbability bias (Shirai & Bettman, 2005)	Social influence (Fischer et al., 2013)	Genre conforming (Luo et al, 2013)	Post-decisional dissonance (Oshikawa, 1969)

These secondary behavioural biases can help us to better understand the tactics of fraudsters. The feeling of **scarcity** makes consumers focus on their unmet needs, which fraudsters exploit.

- **Salience and perception** suggests that individuals are more likely to focus on information that is prominent or emotionally striking. In cases of APP fraud, this materialises when fraudsters use urgent, eye-catching language like "FINAL NOTICE" or "ACCOUNT COMPROMISED" in communications such as emails or text messages. The salience of the warning makes the threat seem more important and real, causing a victim to overlook subtle clues, such as a slightly incorrect email address, that would otherwise signal a fraud.
- **Visceral influence** refers to the way strong "gut feelings" like fear, desire, or anxiety can hijack decision-making, prioritising short-term emotional responses over long-term interests. This is central to romance scams, where a fraudster cultivates feelings of love and dependency. When they create a fake emergency, the victim's visceral fear for the safety of loved ones overwhelms logical scrutiny of the request for money. This is also a feature of impersonation scams, where fraudsters can instill fear through impersonation

of the police, tax authority, employer or other entity which the victim might be fearful of disobeying.

- **Improbability bias** is the tendency to misjudge the likelihood of events, often believing one is unlikely to be the victim of a common event like a scam. A person might receive a fraudulent text and think, "It's probably a scam, but what if it's the one-in-a-million chance that it's real?" This overestimation of a rare event's likelihood can lead them to comply with the fraudulent request "just in case," underestimating the high probability that it is, in fact, a scam.

Fraudsters often exploit natural inclination to **trust** by impersonating credible people or organisations. This is enabled by several underlying biases.

- **Positive affect** describes how being in a good mood can lower critical thinking and increase trust. For instance, a victim might receive a notification that they have won a prize or a small amount of money in an online game. The positive feeling from this "win" makes them more trusting of the platform, and they are therefore more likely to pay a fraudulent "processing fee" to release the non-existent larger prize.
- **Prestige bias** is the tendency to trust and follow the lead of individuals or institutions perceived as having high status or success. Investment scams frequently exploit this by creating fake endorsements from famous entrepreneurs or business leaders. Impersonation scams exploit this by adopting the status of the bank, tax authority, police or an employer, among other institutions with a degree of prestige in the eyes of the victim. In purchase scams, victims see a person they admire seemingly recommending a product and are persuaded by their prestige, leading them to invest without conducting their own due diligence.
- **Social influence** describes how our behaviour is shaped by the actions and opinions of others. Fraudsters manipulate this by creating an illusion of social consensus. For example, a fraudulent cryptocurrency website might feature a live feed of fake testimonials and social media posts from other "investors" who are celebrating their profits. This creates a powerful sense of social proof that the scheme is legitimate and successful, pressuring the victim to join.

The **representativeness heuristic** causes people to judge plausibility based on how much a situation resembles a familiar template, which fraudsters use to make scams look legitimate.

- **Social proof**, a specific type of social influence, is highly relevant here. When a fraudulent e-commerce site displays hundreds of positive product reviews and five-star ratings, it is creating social proof. A potential victim sees this and thinks, "If so many other people had a good experience, it must be legitimate." They rely on the actions of others as a mental shortcut for safety, making them vulnerable to purchase scams.
- The **availability effect** is our tendency to rely on examples that come to mind easily. If a person has recently seen news reports about a particular company, and a fraudster then contacts them with a fake investment opportunity related to that same company, the idea will seem more plausible. The company is "available" in the victim's mind, lending undeserved credibility to the scammer's pitch.
- **Genre conforming** explains our expectation that things should follow established norms or formats. Fraudsters design their phishing emails to conform to the "genre" of an official message from a bank. By using the correct logos, colour schemes, and professional tone, the fake email perfectly matches the victim’s mental model of a real one, leading them to trust it and follow its malicious instructions.

Fraudsters aim to keep their victims in a fast, emotional state of mind (**System 1**) to prevent slow, logical thought (**System 2**).

- The **hot/cool system** model, which is similar to the System 1 / 2 model, describes the tension between an emotional "hot" system that demands immediate action and a logical "cool" system that enables careful thought. Fraudsters trigger the hot system by creating a sense of extreme urgency or panic, for example, by telling a victim their life savings are being stolen at that very moment. The victim's hot system takes over, and they rush to follow the fraudster's instructions to "save" their money, without ever engaging the cool system to question the situation.
- **Impulsivity** is the tendency to act without thinking about the consequences, which fraudsters actively encourage. Fraudsters use tactics which exploit the

impulsivity of their victims and may target individuals who are more likely to be impulsive. A common tactic is a "flash sale" for a high-demand product with a countdown timer. The pressure of the timer is designed to trigger an impulsive purchase. The fear of missing out overrides the normal process of checking the seller's legitimacy, leading directly to a payment for a non-existent item.

- **Post-decisional dissonance** is the discomfort one feels after making a decision, which can lead to seeking out evidence that confirms the choice was correct. After a victim makes a small initial payment in a scam, they might feel doubt. The fraudster then provides fake evidence that the investment is performing well. This resolves the victim's dissonance and confirms their initial decision was a good one, making them highly susceptible to requests for even larger sums of money to chase their "gains".

Behavioural biases and susceptibility to types of APP fraud

Behavioural biases may contribute to susceptibility of consumers to APP fraud, potentially interacting with one another. In this sub-section, we consider how fraudsters might exploit particular biases in specific types of fraud. We consider the main types of fraud (based on UK Finance data from the 2025 Annual Fraud report), which are **purchase, advance fee, impersonation and investment** scams.

Table 2 provides summary statistics on the value and volume of different forms of APP fraud experienced by consumers in 2024. By far the most common type of fraud is purchase scams, which account for 71% of the total volume with 131,447 cases. In terms of financial value, however, investment scams represent the largest losses, totaling £44.4 million or 32% of the total value lost, despite making up only 4% of cases. Impersonation scams are also a major factor, split between police or bank impersonation (£65.9 million) and other forms of impersonation (£35.8 million), which together account for nearly 23% of the total value lost. Other notable categories include romance scams (£30.5 million), advance fee scams (£32.4 million), and invoice or mandate scams (£42.7 million), while CEO fraud accounts for the smallest volume but still results in £11.8 million in losses.

Table 2: Prevalence of Fraud by Type, 2024				
Type of scam	Value (£m)	Volume (N)	Value Share (%)	Volume Share (%)
Purchase	87.1	131,447	19%	71%
Advance fee	32.4	14,749	7%	8%
Impersonation: Other	35.8	17,910	8%	10%
Impersonation: Police / Bank	65.9	7,202	15%	4%
Investment	144.4	7,767	32%	4%
Romance	30.5	4,087	7%	2%
Invoice & Mandate	42.7	2,301	9%	1%
CEO	11.8	270	3%	0%
Source: Reproduced from UK Finance Annual Fraud Report 2025				

Fraudsters might exploit different types of behavioural biases depending on the type of fraud activity they are seeking to engage in. Table 3 below summarises the relevance of the four primary behavioural biases to the most common forms of APP fraud. The table highlights the common theme that corrective action to reduce consumer behavioural vulnerability might reduce multiple forms of fraud. We discuss examples below.

Purchase scams exploit several behavioural biases to appear credible to victims. They strongly leverage the principle of scarcity by presenting products that are either highly discounted, described as "too good to be true," or available as a desirable item on a short-term offer. Trust is partially engaged by associating the scam with a known and trusted brand, even though the vendor itself typically has little to no

platform history or rating. These scams are effective at invoking representativeness, as the product descriptions often include recognised and premium details to make the offer seem genuine. They also prey on System 1 thinking by framing the deal as a short-term opportunity and using pressured interactions. These scams are highly scalable online, simple for fraudsters to imitate, and are designed to mimic a genuine market offer.

Advance fee scams operate by using scarcity to entice victims with the promise of securing an unrealistically cheap or generous product, such as a car or holiday, in exchange for an upfront payment. The role of trust is limited because the vendor is usually not a known brand or trader; instead, fraudsters attempt to build trust through direct interaction with the victim. The scam's representativeness is only partial, as the advance fee requirement can reduce the realism of the offer. Similarly, the use of fast, System 1 thinking is limited because securing payment often requires multiple interactions and a trust-building process. While these scams are highly scalable online, they tend to have a lower conversion rate compared with purchase scams as they cannot exploit behavioural biases relating to time and psychological pressure.

Impersonation scams are based on the manipulation of organisational or societal hierarchies and social capital. They also interact with scarcity, as the impersonator often threatens the victim with loss of resources (in the guise of being HMRC, the police, or some other authority) The primary bias exploited is trust, as the fraudster impersonates a person in a trusted role, such as a CEO, line manager, or an official from the police or HMRC. These scams do not rely on representativeness, as the fraudster usually lacks the detailed information required to appear genuine under close scrutiny. However, they heavily leverage System 1 thinking by commonly portraying the situation as a personal emergency that demands immediate action. These scams are often targeted at a limited number of organisations that have open staff details or contact information available. As such, these scams are not readily scalable.

Investment scams present implausibly high returns and attract those in search of excess returns but also partially use the scarcity principle by attracting consumers who are seeking infeasibly high returns due to lack of saving (e.g., lack of retirement savings). Similar to purchase scams, they rely partially on trust by associating the

product with a known brand, while the vendor themselves has little or no platform history. The use of representativeness is weak because the investment description is often unrealistic and lacks the usual terms, conditions, and disclosure requirements of a legitimate financial product. System 1 thinking is also limited; although the opportunity may be portrayed as oversubscribed, the decision to invest is unlikely to be a quick process. A key feature of these scams is that they have the highest average loss per customer and are often targeted at a higher net worth group of victims. Their lack of scale is compensated for in part by the high value of funds extracted by the average successful scam episode.

Table 3: Behavioural Biases and Susceptibility to APP Fraud Types					
Type of scam	Scarcity	Trust	Representativeness	System 1/2	Other Factors
Purchase	Yes / product tends to be highly discounted, too good to be true, desirable item on short-term offer	Partial / product tends to be a known, trusted brand, though vendor has no or limited platform history/rating	Yes / product has recognised features in description, often premium detail, increasing representativeness	Yes / advert tends to be for short-term available deal, interactions tend to be pressured	Highly scalable online, mimics a genuine market offer, simple to imitate
Advance fee	Yes / advance fee payment to secure unrealistically cheap / generous product e.g. holiday, car	Limited / vendor is not a known brand or trader, attempts to build trust through interaction with the victim	Partial / product realism limited as disclosing need for advance fee reduces representativeness	Limited / securing payment from victim often requires multiple interactions and trust building	Highly scalable online, lower conversion compared with purchase scams
Impersonation	No / scam tends to manipulate organisational or societal hierarchy and social capital within	Yes / trusted person or role within organisation e.g. CEO/line manager, or police, HMRC or other enforcement body	No / fraudster usually lacks detailed information required to appear genuine under scrutiny	Yes / commonly portrayed as a personal emergency or need	Targeted at limited number of organisations with open staff details / contact information
Investment	Partial / attracts consumers who are seeking (infeasibly) high returns	Partial / product tends to be a known, trusted brand, though vendor has no or limited platform history/rating	Weak / investment description is often unrealistic, lacking usual T&Cs and disclosure requirements	Limited / commonly portrayed as an oversubscribed opportunity but unlikely to be a quick choice process	Highest average loss per customer, targets higher net worth victim group

The behavioural biases described in the table are commonly used in combination. The following provides some examples, with the relevant biases referenced in parenthesis:

An online marketplace scam advert for a laptop might describe the laptop as branded (trust), with a detailed description of its features resembling the description one might find in an advert (representativeness). The price may be set at a large discount on the typical purchase price (scarcity), and portrayed as time-limited, in short-supply, and heavily pressured towards the consumer in direct messaging (System 1). This type of scam is highly scalable as online marketplaces can reach large customer volumes.

An advance fee scam to secure a holiday booking might advertise a holiday with a known hotel brand in a highly rated venue (trust), with an itinerary for the holiday which resembles a typical holiday schedule (representativeness). As with the purchase scam, the price may be set at a large discount on the typical purchase price (scarcity), and portrayed as time-limited, in short-supply, and heavily pressured towards the consumer in direct messaging (System 1). This type of scam is less scalable compared to purchase scams but uses many of the same fraud tactics to attract customers.

An impersonation scam attempts to exploit the relationship between the victim and the impersonated individual (trust), but fraudsters have limited ability to authentically imitate the impersonated individual, e.g. the CEO, due to lack of information (representativeness heuristics). This type of scam often relies on emotional, pressured responses (System 1) but is limited in scale as it typically involves one-to-one communication, and (in the example of the CEO scam) relies on obtaining identifying information on employers and employees.

Finally, investment scams might offer high returns (scarcity) in an asset class known for potentially achieving high returns e.g. international property development and purport to offer an investment in a well-known city or location (trust). The property investment might offer details of the location, the properties to be constructed, costs and a timeline (representativeness). This type of scam might emphasise the time-limited nature of the investment (System 1).

5. Insights from behavioural economics for tackling APP fraud

In this section, we discuss how insights from behavioural economics are relevant for tackling APP fraud. The discussion here touches on issues relating to technology of APP fraud (such as payments data, and identification verification), but the focus of the discussion is on how behavioural economics could be used in fraud reduction strategies. We first suggest how behavioural economics informs the types of innovations which could be effective at reducing consumer susceptibility. A common theme in these innovations is challenging the consumer to question the *plausibility* of the fraud scenario the fraudster is attempting to deceive the consumer into. This section does not seek to evaluate current industry or regulatory measures, but considers the relevance of the insights from behavioural economics principles more generally. Payment service providers currently utilise a variety of risk warning approaches and we do not attempt to evaluate these here.

Corrective thinking through behavioural interventions

Remedying the effects of behavioural biases can take a number of forms. Table 4 below outlines the four primary behavioural biases exploited in APP fraud, the corrective thinking required to counter them, and potential interventions to prompt that thinking.

For example, for vulnerability to scarcity, described as susceptibility to offers that are "too good to be true," the evaluation of the offer is distorted by an individual's pressing needs. The necessary corrective thinking is to realise that the offer would be assessed differently in the absence of that need. This could involve resetting the person's decision-making state by raising their self-awareness or by externally communicating the true value of the offer to them.

In cases involving willingness to trust, fraudsters exploit the imitation of entities with a high trust factor. The corrective thought process is to recognise that the person or organisation is an imitation and lacks the credentials or authority they claim to have. One approach could be to prompt individuals to scrutinise the entity's credentials and to question the methods of communication and behaviours being used.

The stereotype bias (representativeness heuristic) involves the overinterpretation of detail as a sign of plausibility. To counter this, an individual needs to engage in

corrective thinking by understanding that the likelihood of the fraudulent claim being true is very low and that the improbable details should be dismissed. A “too good to be true?” challenge may cause them to re-evaluate the situation based on its baseline probability.

Finally, System 1 thinking refers to making decisions in a "hot," emotional state without reasoning. The corrective mindset here is the recognition that in a more reflective state, the fraudulent offer would be dismissed as inauthentic because its features are dubious upon reflection. This may be achieved by either slowing down the choice process or, while maintaining the speed, increasing the share of time that is dedicated to reflection and verification.

The existence of these biases, and the need for corrective thinking, is not limited to APP fraud but may occur in many contexts. Out of vulnerability to scarcity a business owner struggling to keep trading might take a business loan out of desperation based on unrealistic expectations of turning around the business. Willingness to trust can be exploited by brands who recruit high-trust individuals to front their marketing campaigns and imbue trust in their products by association. The representativeness heuristic might cause individuals to buy a book based on the cover image and blurb thinking it resembles a genre they enjoy, only to find once they begin reading that it does not. System 1 thinking is exploited by sales and marketing in multiple domains.

In the APP context, there are common themes in the corrective thinking required to reduce susceptibility to behavioural biases. First, corrective thinking requires the consumer to re-evaluate the prospect to consider whether it is plausibly true. This might be a price which is too good to be believable (overcoming the vulnerability to scarcity and stereotype bias - representativeness heuristic), or the plausibility of the credentials of an impersonator. Second, and relatedly, the corrective thinking to re-evaluate requires some extent of deliberation and the associated delay. This is particularly relevant to APP fraud exploiting scarcity and System 1 thinking, in which the consumer is pressured into a fast decision (e.g., for an apparently short-term deal) of a product, service or prospect (e.g., a romantic relationship) which is too good to be true or apparently pivotal on some fast decision (e.g., the transfer of some emergency funds to a romantic partner in some emergency scenario).

Table 4: Behavioural Insights into Potential Interventions		
Behavioural bias	**Corrective thinking**	**Potential mechanisms**
Vulnerability to scarcity: susceptibility to “too good to be true” (e.g. Shah et al., 2015):	The evaluation of the fraudulent good/service being offered is distorted by the high needs of the individual. It would be evaluated differently absent the need.	Resetting the decision state of the individual by raising self-awareness. External communication of true value of the offer to the individual.
Willingness to trust: imitation of agents with high trust factor (e.g. Chang & Chong, 2010)	Individual / organisation is not to be trusted but is imitating a real entity. They do not have the credentials or authority they claim to have.	Prompt individuals to scrutinise the credentials of the individual / organisation, and question the mode of communication and behaviours.
Representativeness heuristic: overinterpretation of detail as plausibility (e.g. Tversky & Kahneman, 1974)	The likelihood of the claim to authenticity being true is very low. The claimed detail and social proof attached to the fraud is improbable and should be dismissed.	Confront individuals with a “too good to be true?” challenge which causes them to evaluate the likelihood (re-orientate their evaluation to the baseline probability).
System 1 thinking: making decisions in a “hot” state without reasoning (Kahneman, 2011)	In a reflective thinking state, an evaluation of the fraudulent good/service being offered would dismiss authenticity. The claimed features of the offer, on reflection, are dubious.	Slowing down the choice process, or maintaining the speed of the choice process but increasing the share of time dedicated to reflection and verification.

Behavioural design considerations

In designing behavioural remedies, the need to move the consumer into a state of **re-evaluation** and **deliberation & delay** is not the only consideration. As is commonly the case in the design of behavioural remedies, there is a trade-off between multiple outcomes of interest. The majority of payments are for non-fraudulent, legitimate money transfers and there are costs associated with slowing or stopping these payments. Behavioural remedies should seek to reduce "illegitimate" payments which are associated with fraud, while maintaining or increasing the completion of "legitimate" payments. The literature and behavioural economics toolkit suggests that the effectiveness of risk warnings may vary depending upon factors including:

- **Risk-based approaches**: When designing behavioural interventions to combat APP fraud, a key consideration is the use of risk-based approaches and potentially even a "less is more" targeting strategy. The challenge with prompting the consumer to deliberate and delay is that the majority of payments are known to the consumer to be legitimate and routine, and there is a risk that over-prompting with warnings and interventions could render warnings less effective by creating cognitive fatigue and muscle memory effects. Warnings and interventions could aim to heighten consumer diligence specifically in scenarios involving payments that are deemed risky. This approach has already been proposed in the authorised payments space (Akesson et al., 2023). However, the effectiveness of risk-based approaches may depend on the method of targeting, the content of those warnings in relation to the behavioural biases they seek to mitigate, and their effectiveness when consumers are exposed to them repeatedly. The likelihood that a payment is fraudulent varies greatly depending on payee characteristics, the payment reason, and the value of the transaction. Therefore, targeting warnings and interventions based on these factors may yield a net benefit by successfully preventing fraudulent payments while minimising friction and disruption for the vast majority of legitimate payment journeys.

- **Decision making contexts and “just-in-time” warnings.** The context of the user's decision-making process and the timing of any intervention may also be important. For instance, whether remedies are deployed on the online marketplace, platform, or messaging service where the fraudulent good or service is being marketed, or later during the payment stage. Some studies have noted that at the payment stage some individuals may be psychologically committed to their choice and keen to complete the transaction quickly to minimise the “pain of paying” (Prelec & Loewenstein, 1998; Quispe-Torreblanca et al., 2019). “Just-in-time” warnings may be another type of intervention, based on multi-dimensional characteristics of the payment and the specific decision environment where the fraud originates, such as the messaging app, or marketplace. Just-in-time warnings have been shown to be effective in a variety of domains (Nahun-Shani et al., 2018).

- **Heterogeneity in susceptibility.** There is heterogeneity in susceptibility to fraud across different individuals. Susceptibility can vary based on measurable characteristics including age, financial literacy, and digital literacy. In addition, self-awareness of both vulnerability to and exposure to fraud may vary across individuals. These traits may therefore indicate which individuals may have the greatest potential to benefit from interventions that, for instance, increase their diligence by raising self-awareness of their perceived vulnerability to scams. Indeed, previous evidence from Decision Lab (2023) suggests that a self-audit exercise in the form of a personal financial risk assessment resulted in reduced susceptibility to fraud within a hypothetical setting.

Technological design considerations

In the context of behavioural remedies, the design and testing environment is also a relevant consideration. Recent innovations have been achieved in how behavioural interventions can be developed and evaluated using new technologies. These approaches could potentially help reduce the costs associated with innovation while

improving the realism of development and testing. Below, we discuss these innovations and their relevance to behavioural economics research in APP fraud.

- **Survey-based experiments**. Behavioural economics is making increased use of survey-based experiments, which replicate online consumer journeys and can be used to test interventions (as in Akesson et al., 2023). These experiments offer internal validity via an incentive-compatible design in which participants are rewarded with an incentive structure reflecting the incentives facing consumers in real-world settings. They also offer a higher degree of environmental validity than can be achieved in other settings due to the capacity to design online banking payments journeys in experimental settings which capture the key features of real-world journeys. These environments lend themselves to the testing of interventions focused on targeted, risk-based approaches. They also permit the creation of multiple online environments (such as purchase environments and payment environments), facilitating testing of interventions in multiple decision-making contexts.

- **Survey-linked transaction data**. Studies in behavioural economics also increasingly draw on linked data sources. This is implemented by integrating a survey platform with an open banking partner to access transaction data. This design's advantage is its ability to combine survey features like subjective responses and hypothetical questions with real-world, objective transaction measures. Its disadvantage can be that samples tend to be skewed towards users of open banking. However, there is likely to be a positive correlation between use of payment technologies such as open banking, and use of push-payments to acquire goods and services, hence overlap in the relevant research population. These data can be valuable for linking survey-measures of vulnerability to transaction-based measures of heterogeneity in susceptibility.

- **Survey-based instruments.** Behavioural economics also increasingly adopts survey-based instruments which aid the measurement of behavioural biases and other behavioural characteristics. For example, Dohmen et al. (2005) developed a range of survey items for the measurement of risk which can be

deployed using minimal space in the survey. More recently, Stango & Zinman (2023) deploy a range of survey questions designed to measure a suite of behavioural biases in survey data. The advantages of this method include the use of representative samples and the capacity to flexibly add questions between waves or conduct standalone surveys.

6. Conclusion

Authorised Push Payment (APP) fraudsters systematically exploit known human vulnerabilities to achieve their aims. Behavioural economics provides a lens through which to view the activity of fraudsters as exploiting behavioural biases, primarily among which are vulnerability to scarcity, willingness to trust, susceptibility to the representativeness heuristic and System 1 vs System 2 thinking. This report has described how these biases make consumers susceptible to fraud, and how secondary behavioural biases are also at work in consumer vulnerability.

Behavioural economics may, however, provide insights into potential behavioural interventions. The aim of interventions is to mitigate behavioural bias by prompting the consumer to deliberate and delay over their choice decision. While this might naturally lead to the design and implementation of risk warnings and frictions in the payments process, interventions also need to account for the cognitive fatigue and context-specific pressures that warnings themselves may create. They also need to consider that there are financial and economic costs to slowing legitimate transactions, and so design interventions in such a way as to maximise the payment of legitimate transactions while minimising the payment of illegitimate transactions.

This report suggests three potential behavioural design considerations inspired by the academic literature: risk-based approaches, consideration of decision-making contexts and “just-in-time warnings”, and heterogeneity in vulnerability across consumers. It also discusses how technological innovations in survey-based experiments, survey-linked transaction data and survey-based instruments facilitate investigation of potential interventions with high degree of internal and environmental validity, improving the external validity of intervention designs.

Bibliography

Akesson, J., Gathergood, J., & Quispe-Torreblanca, E. (2023). Preventing payments fraud in the FinTech era: New evidence from a behavioural experiment (No. 2023-08). CeDEx Discussion Paper Series.

Arrow, K. J., & Debreu, G. (1954). Existence of an equilibrium for a competitive economy. *Econometrica, 22*(3), 265–290.

Behavioural Insights Team. (2012). *Behavioural insights team annual update 2011-12*. Cabinet Office.

Behaviouralist, The (2021) Using behavioural insights and experimentations to prevent APP fraud. Report prepared for Open Banking Ltd.

Beshears, J., Blakstad, M., Choi, J. J., Firth, C., Gathergood, J., Laibson, D., ... & Stewart, N. (2024). Does pension automatic enrollment increase debt? Evidence from a large-scale natural experiment (No. w32100). National Bureau of Economic Research.

Braga, J. N., Ferreira, M. B., Sherman, S. J., Mata, A., Jacinto, S., & Ferreira, M. (2018). What's next? Disentangling availability from representativeness using binary decision tasks. *Journal of Experimental Social Psychology*, 76, 307-319.

Camerer, C. F., Dreber, A., Forsell, E., Ho, T. H., Huber, J., Johannesson, M., ... & Wu, H. (2016). Evaluating replicability of laboratory experiments in economics. *Science*, 351(6280), 1433-1436.

Camerer, C. F., & Loewenstein, G. (2006). Behavioral economics. Econometric Society Monographs, 42, 181.

Chang, J. J., & Chong, M. D. (2010). Psychological influences in e-mail fraud. *Journal of Financial Crime*, 17(3), 337-350.

Cribb, J., & Emmerson, C. (2016). What happens when employers are obliged to nudge? Automatic enrolment and pension saving in the UK (No. W16/19). IFS Working Papers.

Dambe, K., Hunt, S., Iscenko, Z., & Brambley, W. (2013). Applying behavioural economics at the Financial Conduct Authority. FCA Occasional paper, (1).

Decision Lab (2023) “Protecting Older Investors From Financial Fraud” last accessed via https://thedecisionlab.com/case-study/protecting-older-investors-from-financial-fraud, 20th June 2025

DellaVigna, S. and E. Linos (2022). RCTs to scale: Comprehensive evidence from two nudge units. *Econometrica* 90(1), 81–116.

Dohmen, T., Falk, A., Huffman, D., Sunde, U., Schupp, J., & Gert, G. W. (2005). Individual risk attitudes: New evidence from a large, representative, experimentally-validated survey (No. 511). DIW Discussion Papers.

Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., & Vlaev, I. (2012). Influencing behaviour: The mindspace way. *Journal of Economic Psychology*, 33(1), 264-277.

Financial Conduct Authority. (2014). CP14/10. *Proposals for a price cap on high-cost short-term credit*. Financial Conduct Authority

Financial Conduct Authority. (2018). *PS18/4: Credit card market study: Persistent debt and earlier intervention - feedback to CP17/43 and final rules*. Financial Conduct Authority.

Financial Conduct Authority (2020). CP20/19. *General insurance pricing practices market study*. Financial Conduct Authority.

Financial Conduct Authority. (2021). *PS22/10: Strengthening our financial promotion rules for high-risk investments and firms approving financial promotions*. Financial Conduct Authority.

Financial Conduct Authority. (2022). *CP22/20: Sustainability disclosure requirements (SDR) and investment labels*. Financial Conduct Authority.

Financial Conduct Authority. (2023). *PS23/6: Financial promotion rules for cryptoassets.* Financial Conduct Authority.

Financial Conduct Authority. (2024). *Occasional paper 66: Playing the market: A behavioural data analysis of digital engagement practices and investment outcomes*. Financial Conduct Authority.

Finn, P., & Jakobsson, M. (2007). Designing ethical phishing experiments. *IEEE Technology and Society Magazine*, *26*(1), 46-58.

Fischer, P., & Greitemeyer, T. (2013). The positive bystander effect: Passive bystanders increase helping in situations with high expected negative consequences for the helper. *Journal of Social Psychology*, *153*(1), 1-5.

Friedman, M. (1953). *Essays in positive economics*. University of Chicago Press.

Gathergood, J., Guttman-Kenney, B., & Hunt, S. (2019a). How do payday loans affect borrowers? Evidence from the UK market. *Review of Financial Studies*, 32(2), 496-523.

Gathergood, J., Mahoney, N., Stewart, N., & Weber, J. (2019b). How do individuals repay their debt? The balance-matching heuristic. *American Economic Review*, 109(3), 844-875.

Gathergood, J., Hirshleifer, D., Leake, D., Sakaguchi, H., & Stewart, N. (2023). Naive buying diversification and narrow framing by individual investors. *Journal of Finance*, 78(3), 1705-1741.

Hume, D., Gathergood, J., & Stewart, N. (2024). The Limits of Nudge: Evidence from Online Property Listings. Available at SSRN 4846383.

Judges, R. A., Gallant, S. N., Yang, L., & Lee, K. (2017). The role of cognition, personality, and trust in fraud victimization in older adults. *Frontiers in Psychology*, 8, 588.

Kahneman, D. (2011). *Thinking, fast and slow*. Farrar, Straus and Giroux.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*(2), 263–291.

Langenderfer, J., & Shimp, T. A. (2001). Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing, 18*(7), 763–783.

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28-38.

Metcalfe, J., & Mischel, W. (1999). A hot/cool-system analysis of delay of gratification: Dynamics of willpower. *Psychological Review, 106*(1), 3–19.

Nahum-Shani, I., Smith, S. N., Spring, B. J., Collins, L. M., Witkiewitz, K., Tewari, A., & Murphy, S. A. (2018). Just-in-time adaptive interventions (JITAIs) in mobile health: key components and design principles for ongoing health behavior support. *Annals of Behavioral Medicine*, 1-17.

Ong, A. S. (2022). Think first, act later, or act first, think later: Does the fraud triangle hold when individuals are impulsive?. *Journal of Forensic and Investigative Accounting*, 14(1), 11-38.

Oshikawa, S. (1969). Can cognitive dissonance theory explain consumer behavior?. *Journal of Marketing*, 33(4), 44-49.

Prelec, D., & Loewenstein, G. (1998). The red and the black: Mental accounting of savings and debt. *Marketing Science*, 17(1), 4-28.

Quispe-Torreblanca, E. G., Stewart, N., Gathergood, J., & Loewenstein, G. (2019). The red, the black, and the plastic: paying down credit card debt for hotels, not sofas. *Management Science*, 65(11), 5392-5410.

Roethke, K., Klumpe, J., Adam, M., & Benlian, A. (2020). Social influence tactics in e-commerce onboarding: The role of social proof and reciprocity in affecting user registrations. *Decision Support Systems*, 131, 113268.

Samuelson, P. A. (1947). *Foundations of economic analysis*. Harvard University Press.

Schmidt, U., & Zank, H. (2005). What is loss aversion?. *Journal of Risk and Uncertainty*, 30, 157-167.

Shah, A. K., Shafir, E., & Mullainathan, S. (2015). Scarcity frames value. *Psychological Science*, *26*(4), 402-412.

Shirai, M., & Bettman, J. R. (2005). Consumer expectations concerning timing and depth of the next deal. *Psychology & Marketing*, *22*(6), 457-472.

Simon, H. A. (1955). A behavioral model of rational choice. *Quarterly Journal of Economics, 69*(1), 99–118.

Simon, H.A. (1990). Bounded Rationality. In: Eatwell, J., Milgate, M., Newman, P. (eds) Utility and Probability. The New Palgrave. Palgrave Macmillan, London

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2007). The affect heuristic. *European Journal of Operational Research, 177*(3), 1333–1352.

Stango, V., & Zinman, J. (2023). We are all behavioural, more, or less: A taxonomy of consumer decision-making. *Review of Economic Studies*, 90(3), 1470-1498.

Thaler, R. H. (1980). Toward a positive theory of consumer choice. *Journal of Economic Behavior & Organization, 1*(1), 39–60.

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press.

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases: Biases in judgments reveal some heuristics of thinking under uncertainty. S*cience*, *185*(4157), 1124-1131.

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. science, 211(4481), 453-458.

Tversky, A., & Kahneman, D. (1990). Judgment under uncertainty: Heuristics and biases.

UK Finance. (2025). *Annual fraud report 2025*. UK Finance.

Zhang, W., Luo, X., Burd, S. D., & Seazzu, A. F. (2012, January). How could I fall for that? Exploring phishing victimization with the heuristic-systematic model. In 2012 45th *Hawaii International Conference on System Sciences* (pp. 2374-2380). IEEE.

Appendix 1: Typology of APP Fraud

Purchase Scam: This is the most common type of APP fraud by volume. It occurs when a victim pays for goods or services that are never delivered or are worthless. Example: A person sees an advertisement on social media for a high-demand item, such as a games console or a specific breed of pet, at a discounted price. They transfer the money directly to the seller, who then ceases all contact and never sends the item.

Advance Fee Scam: This fraud involves tricking a victim into paying a fee upfront with the promise of receiving a larger sum of money, a valuable prize, or a loan later, which never materialises. Example: A victim receives an email informing them they have won an international lottery. To receive their winnings, they are told they must first pay a fee to cover "taxes and processing," after which they will receive nothing.

Impersonation - Police / Bank Scam: This happens when a fraudster contacts a victim pretending to be from an authority figure, such as their bank's fraud department or the police, to gain their trust and trick them into making a payment. This type of scam accounts for 15% of the total value lost to APP fraud. Example: A criminal calls a victim, claiming to be from their bank's fraud team. They state that the victim's account has been compromised and that to protect their money, they must immediately transfer their entire balance to a new "safe account" provided by the caller, which is actually an account controlled by the fraudster.

Impersonation - Other: This is a broad category of impersonation scams where the fraudster pretends to be from other trusted organisations that are not the police or a bank. Example: A person receives a text message appearing to be from a parcel delivery company, stating they need to pay a small "redelivery fee" for a package. The link directs them to a fake website that harvests their payment details.

Investment Scam: This type of fraud results in the highest financial losses, accounting for 32% of the total value. It involves persuading a victim to move their money into a fictitious fund or to pay for a worthless or non-existent investment opportunity. Example: A victim is targeted with online adverts for an investment in cryptocurrency or rare metals that promises fast, guaranteed high returns. They are directed to a professional-looking but fake trading platform where they make an initial

investment. The fraudsters show them fake profits to encourage them to invest more, before eventually ceasing contact and taking all the money.

Romance Scam: Fraudsters build a relationship with their victim, often online over a period of time, to gain their affection and trust before asking for money for fictitious reasons. Example: A person on a dating app develops what feels like a genuine long-distance relationship. After gaining their trust, the fraudster invents a crisis, such as a medical emergency or a problem with their business, and asks the victim to send them money to help, with no intention of paying it back.

Invoice & Mandate Scam: This typically targets businesses and involves tricking them into changing the bank account details for a payment to a legitimate supplier. The fraudster provides their own account details instead. Example: An employee in a finance department receives an email that appears to be from one of their regular suppliers, stating that they have new bank details. The employee updates the payment information, and the next payment for a legitimate invoice is sent to the fraudster's account instead of the supplier's.

CEO Scam: A fraudster impersonates a senior executive within the victim's own organisation to instruct an employee to make an urgent, confidential payment. Example: An employee in the finance team receives an email that looks like it is from their company's CEO. The email stresses urgency and secrecy, instructing the employee to immediately process a wire transfer to a foreign account to secure a "confidential acquisition." The employee, believing the request is a legitimate order from their boss, makes the payment.

Axiom Economics

London