Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Research Technical Paper

Caught in the Net: Patterns and Predictors of Fraud Incidence in Ireland

Danish Us-Salam, Anu Jose & Jane Kelly

Vol. 2026, No. 7

Caught in the Net: Patterns and Predictors of Fraud Incidence in Ireland [*]

Danish Us-Salam[1], Anu Jose[1,2], and Jane Kelly[1]

[1]Central Bank of Ireland
[2]University of Galway

Abstract

Fraud and scams are an increasingly complex and global challenge, yet evidence on their impact on individuals remains limited. Using a broadly nationally representative survey of nearly 3,000 adults in Ireland, this study maps consumer fraud journeys, including whether individuals are targeted, whether they lose money, and what follows in terms of reporting and recovery. More than one in three respondents reported experiencing fraud, and almost two-thirds of these individuals lost money as a result. A prediction exercise shows that the likelihood of experiencing fraud is strongly influenced by behavioural factors, while demographic characteristics such as age, education, or income also play a role. Fraud-specific literacy significantly reduces predicted fraud experience, whereas general financial literacy does not. Greater use of digital and financial products increases predicted fraud experience. Risky online behaviours—including shopping on unfamiliar websites, sharing payment details through insecure channels, and sending money to unknown individuals—emerge as the strongest behavioural predictor of fraud experience. These results highlight the rationale for current multi-faceted and cross-agency approaches, which seek to improve public awareness and education specific to fraud, while also strengthening digital and financial system safeguards.

Keywords: Fraud Incidence, Fraud Literacy, Risky Online Behaviour, Financial Vulnerability.
JEL codes: D14, D18, G53, K42, G41

[*]We appreciate participants at the Central Bank of Ireland (CBI) Econ Seminar and internal policy personnel within the bank for helpful suggestions and comments. The views expressed herein are those of the authors and do not necessarily reflect the views of the Central Bank of Ireland.

Non-technical Summary

Tackling frauds and scams is a key priority for policymakers and industry internationally, with losses exceeding $1 trillion globally in 2024 (Alliance and Feedzai, 2024). In Ireland, total payment related fraud reached €160 million in 2024, with losses as a result reaching €66 million (CBI, 2025). This study provides new and detailed insights on consumers' fraud experiences in Ireland. It also extends the literature on fraud risk factors, by studying the consumer behaviours and financial characteristics that may influence consumers' vulnerability to fraud in an increasingly digital era.

We conducted an online survey with 2,945 adults in Ireland between December 2024 and January 2025. The sample was selected to be broadly nationally representative. First, we document the share of consumers in Ireland who have experienced fraud, the types of fraud they experience, typical amounts lost, whether they reported the fraud and were able to recover their funds. Second, we investigate the relationship between those who report experiencing fraud and characteristics such as financial literacy, fraud literacy, and risky online financial behaviours, in addition to the traditional demographic characteristics that have been the main focus of previous studies. We find that more than one-third of consumers in Ireland report experiencing fraud. Online purchase fraud is the most common type of fraud experienced. Further, the majority of individuals affected by fraud report suffering monetary losses of below €250. However, we observe that 38% of those who experience fraud did not report the incident to any authority. We find lower recovery rates among those who do not report the fraud, as well as divergent recovery rates across different types of fraud.

Demographic factors like age, education, and income matter in explaining the likelihood of fraud experience. However, we demonstrate that risky online behaviours and financial characteristics are more strongly correlated with fraud experience. Higher usage of digital and traditional financial products increases fraud incidence, while risky online behaviour is the single strongest predictor of fraud experience. We demonstrate that fraud literacy is correlated with lower fraud experience, whereas general financial literacy is not. Our results suggest that experiencing fraud is common among consumers in Ireland. It points to the importance of targeted prevention strategies that combine safeguards from a financial system perspective with enhanced consumer education and awareness around fraud specifically, as opposed to more general financial literacy.

1 Introduction

Fraud and scams pose a central policy challenge. They have the potential to erode consumer confidence and hinder the operational resilience of the financial system, particularly in an era of rapid financial innovation and digitalisation (Balakrishnan et al., 2025; Europol, 2025; EBA, 2025b). Global losses from fraud and scams are substantial, exceeding $1 trillion in 2024 (Alliance and Feedzai, 2024). Based on data collected from 60 jurisdictions globally, 85% identify fraud and scams as the top risk facing consumers (OECD, 2026). Within Europe, a joint publication by the European Banking Authority and the European Central Bank reported €4.3 billion in fraudulent payments in the European Economic Area (EEA) in 2022 and an additional €2.0 billion in the first half of 2023 (EBA and ECB, 2024).[1] Beyond the direct financial harm, fraud also imposes lasting psychological costs and undermines trust in financial institutions (Brenner et al., 2020; Gurun et al., 2018; Lourie et al., 2023).

Ireland broadly aligns with these global trends. Central Bank of Ireland statistics indicate that total payment fraud reached €160 million in 2024, up 24.5% from 2023. Nevertheless, fraud accounts for a relatively small share of overall payment activity, affecting approximately one in every 10,000 payment transactions (CBI, 2025). At the same time, consumer-facing evidence points to substantial individual-level risk. Research by Banking & Payments Federation Ireland (BPFI) finds that 20% of regular online shoppers experienced financial losses due to scams between November 2023 and 2024, with some individuals losing hundreds or even thousands of euros (BPFI Core Research, 2024). This highlights the significant impact frauds and scams can have on consumers' day-to-day financial lives despite its low incidence at the aggregate level.

For policymakers, combating fraud is an ongoing challenge, with theft or breach of customer credentials, social engineering, and artificial intelligence amplifying criminals' effectiveness in targeting consumers (Europol, 2024, 2025; EBA, 2025a). Despite these developments, detailed consumer-level evidence on fraud incidence and its consequences remains scarce. Identifying who is most at risk and the factors driving their exposure can be critical for informing targeted prevention strategies and effective policy responses.

In response to this knowledge gap, we draw on a sample that was selected to be broadly nationally representative to provide new insights into consumer susceptibility to frauds and scams in Ireland. Our study examines the types of fraud experienced, amounts lost, reporting behaviours, and recovery outcomes. We then analyse the correlation between consumers' financial characteristics and behaviours and their predicted fraud

[1] However, fraud as a share of the total value of payment transactions remains low.

experience. We consider financial literacy, fraud literacy, usage of digital and non-digital financial products, and risky online financial behaviours, alongside demographic factors.

Our evidence shows that fraud incidence in Ireland is common and consequential. More than one-third of consumers report having experienced fraud. Online purchase scams are the most common, followed by debit & credit card fraud, with other types of fraud also prevalent including impersonation of a delivery service and phishing or email scams. The majority of affected individuals report suffering relatively small monetary losses. Approximately 37% report no monetary losses, 39% lost less than €249, while around 10% lost between €250 and €499. However, 38% of individuals who experience fraud did not report the incident to any authority, and there is a striking difference in recovery rates among those who report and those who don't. Engagement with formal channels is strongly associated with better financial outcomes after fraud - 57% of those who lost money and reported it were able to recoup funds, while 13% of non-reporters recovered funds. Recovery was also dependent on the type of fraud. Recovery rates were higher for debit and credit card fraud than for other types of fraud. While most losses were relatively modest in scale, the prevalence of fraud, combined with underreporting to authorities, highlights the challenge facing policymakers.

Beyond prevalence, our prediction analysis demonstrates that behavioural and financial characteristics predict the experience of fraud along with socio-demographic characteristics. Fraud literacy predicts lower fraud experience, but general financial literacy does not. By contrast, greater use of digital and traditional financial products predicts fraud experience, while risky online behaviour emerges as the single strongest predictor of fraud experience. These results suggest that consumer vulnerability is shaped by how individuals interact with financial products and digital environments as well as by their socio-demographic characteristics. It highlights the importance of targeted prevention strategies that combine behavioural insights and education with system safeguards.

This study contributes to the growing literature on evidence-based consumer protection strategies related to fraud and scams in two ways. First, it provides a comprehensive and systematic account of consumer fraud experiences. It examines not only whether individuals have experienced fraud but also whether they incurred financial losses, reported the incident, and ultimately recovered funds. By capturing this full sequence of outcomes, our analysis goes beyond aggregate prevalence rates to show how fraud unfolds in practice. It highlights the points at which regulatory and institutional interventions can be effective. In doing so, we complement industry and administrative records on fraud and scams (BPFI, 2024; Varadarajan, 2025). We also provide a systematic consumer perspective that is often missing in earlier surveys (Permanent TSB, 2024; Houtti

et al., 2024; BPFI, 2019a,b; Wise, 2024; BPFI Core Research, 2024; B&A, 2023).

Second, by linking fraud experience to a comprehensive range of financial characteristics and behaviours, our analysis offers a deeper understanding of the mechanisms underlying fraud susceptibility. Prior research has primarily emphasised demographic and socio-economic risk factors such as age, income, education, and technological literacy (Ross et al., 2014; Lokanan and Liu, 2021; Koning et al., 2024; DeLiema et al., 2023). Even when financial dimensions have been considered, the focus has typically been narrow, centring on financial literacy or risk profiles (Xiao et al., 2022; Deliema et al., 2020). Our study expands these approaches by examining a broad range of financial characteristics. This includes examining whether fraud literacy translates into lower prevalence, and exploring how a spectrum of everyday risky online financial practices shapes susceptibility.

Our findings have direct policy relevance for regulators, law enforcement agencies and industry. For instance, our findings on under-reporting of fraud to authorities point to the need to educate consumers about the urgency of reporting and to make reporting processes as simple as possible for consumers. For instance, minimising the steps required to report fraud and making sure the process is accessible for all, including those with lower digital literacy skills. The results on fraud literacy provide empirical support for initiatives which aim to enhance consumer awareness of common fraud symptoms, such as the Central Bank of Ireland's consumer awareness campaigns.[2] Our results also demonstrate a strong correlation between risky online behaviours and fraud experience, providing a compelling rationale to improve consumer awareness of what constitutes risky online behaviours. For example, BPFI (2025) finds that fewer than one-third of consumers in Ireland take basic online security precautions, such as verifying website authenticity. Such educational efforts will be needed to complement system-level safeguards, including anomaly detection and IBAN verification, to help mitigate consumer vulnerability.[3]

[2] The Central Bank of Ireland's fraud literacy initiatives include media campaigns such as 'Can you spot a scam artist?' and a list of unauthorised firms. The Competition and Consumer Protection Commission, the Garda and many financial institutions including Fraudsmart also raise awareness and offer tools such as SCAMCHECKER.IE.

[3] For example, the EU Payment Services Directive 3 (PSD3) should strengthen system safeguards by requiring mandatory IBAN/name checks whereby a payment is only completed after verification by the bank that the name on the account 'matches' the IBAN linked to that name.

2 Fraud and Scams Incidence: Global and Irish Trends

Recent evidence on the prevalence and losses from fraud and scams globally highlights the growing risk to consumers.[4] In the US, the Federal Trade Commission reports that consumer fraud losses increased by 25% in 2024, reaching $12.5 billion (Federal Trade Commission, 2025a). In the UK, gross fraud losses before recovery totalled £1.17 billion in 2024, broadly unchanged in value terms, but the number of fraud cases rose by 12% compared with 2023 to reach 3.31 million (UK Finance, 2025).

In Ireland, while fraud remains a relatively small share of overall payment activity, Central Bank of Ireland statistics show that total value of fraudulent payments rose by 24.5% in 2024 compared to 2023 (Central Bank of Ireland, 2025). Fraudulent credit transfers using Strong Customer Authentication (SCA) increased from 53% in 2023 to 62% in 2024, suggesting a growing shift towards methods that exploit consumer behaviour rather than technical vulnerabilities alone. It also underscores the importance of complementing system-level safeguards with consumer-facing education and behavioural interventions.

In the UK, unauthorised card fraud, particularly remote purchase fraud (34%), accounted for the biggest share of gross fraud losses in 2024, while investment fraud also accounted for a sizeable proportion (12%) (UK Finance, 2025). In the US, the most frequently reported frauds in 2024 included impersonation scams, online shopping fraud, business and job opportunity scams, investment fraud, and internet service fraud (Federal Trade Commission, 2025b).

Across major economies, cyber-enabled fraud is growing with online fraud accounting for between 20% and 50% of reported cases in most countries, although phone, text and email fraud remain substantial (Global Anti-Scam Summit, 2025, (Europol, 2024; UK Finance, 2025)). In the UK, digital fraud accounted for 50% of all online crime, and it is estimated that 70% of Authorised Push Payment (APP) fraud cases began online (UK Finance, 2025).[5] In Ireland, 77% of the value of fraudulent payments occurred online (Central Bank of Ireland, 2025). The international nature of online fraud emphasises the importance of collaboration across borders and industries.

[4] Even though 'fraud' and 'scams' are often used interchangeably, fraud broadly involves 'unauthorised' access to personal information that results in financial loss (such as when cards or account details are stolen), whereas scams rely primarily on deception and manipulation of the victim, rather than on breaching systems or stealing credentials.

[5] Authorised push payment fraud occurs when the account holder is tricked into authorising a payment to a fraudster, often through social engineering.

Similar to industry and regulatory evidence on aggregate losses and fraud typologies, consumer surveys globally point to a high level of direct exposure to fraud and scams. In the United States, a Pew Research Center survey finds that a majority of adults report receiving scam phone calls (68%), emails (63%), or text messages (61%) at least weekly that attempt to obtain personal information (Pew Research Center, 2025). In the UK, 14% of adults reported experiencing a fraud or scam related to banking, payments, pensions, and/or investments between May 2023 and 2024 (Financial Conduct Authority, 2024). The report also highlights active consumer precautionary behaviour in the UK, with 72% rejecting or ignoring unsolicited contacts, 68% regularly checking bank and credit card statements, and 62% avoiding unexpected web links.

Survey evidence in Ireland is consistent with these international patterns. The Banking and Payments Survey Ireland 2025 indicates that 58% of consumers encountered scam text messages, 52% scam phone calls on mobile phones, and 48% scam emails (BPFI, 2025). The Competition and Consumer Protection Commission reported in 2022 that 20% of consumers had experienced fraud in the preceding year (Competition and Consumer Protection Commission, 2023), while a separate survey by Permanent TSB found that approximately 14% of consumers had been affected by fraud (Permanent TSB, 2024). Despite this growing body of evidence, there remains a lack of systematic data on the full sequence of consumer fraud experiences— from exposure, through the types of scams encountered and the extent of financial loss, to recovery outcomes and reporting behaviour.

3 Data

We study consumer-level fraud patterns in Ireland. We use survey data collected in December 2024 – January 2025, comprising 2,945 respondents. The sample was selected to be broadly nationally representative, based on age, gender, social class, and region. Table 1 provides the sample distribution across various demographic characteristics and a comparison to Irish population statistics.

Overall, the differences between the population benchmarks and the survey sample are relatively small. Gender composition is close to national figures. Females account for 56% of the sample compared with 51% of the population. Age groups are generally well represented, though some deviations are evident. Younger adults aged 18–24 are underrepresented in the sample (4% versus 11% in the population). Individuals aged 65 and over are also underrepresented (13% versus 19%). By contrast, middle-aged groups, particularly those aged 35–54, are somewhat overrepresented relative to pop-

ulation shares. Social grade classifies individuals by occupation and employment status. This ranges from higher professional and managerial roles (AB) through intermediate and skilled occupations (C1 and C2) to semi-skilled, unskilled, and non-working groups (DE and F), and shows more pronounced differences. Higher social grades (AB and C1) are overrepresented in the sample, while lower social grades (DE and F) are underrepresented relative to population benchmarks. Finally, the regional distribution closely mirrors national patterns. Dublin accounts for 28% of the sample compared with 29% of the population. The remaining respondents are distributed across the rest of Leinster, Munster, and Ulster/Connacht in proportions that closely align with population shares.

While some of these differences are non-trivial, particularly for age and social grade, they are broadly in line with patterns commonly observed in online survey samples. Importantly, no single demographic group is absent or overwhelmingly dominant, and the sample retains substantial coverage across all key population segments. As such, the deviations are unlikely to materially bias the descriptive or regression based analysis. To further address any remaining concerns around sample composition, all main analyses are re-estimated using population weights constructed from the demographic benchmarks in Table 1. The weighted results are quantitatively and qualitatively very similar to the unweighted estimates, with no changes to the direction, magnitude, or statistical significance of the key findings. This provides reassurance that the results are not driven by sample composition and are robust to reweighting.

Some limitations may nonetheless apply. Our online survey, while broadly representative given almost universal internet access (95%) among Irish households (CSO, 2025), may not fully capture less digitally active groups such as the over 75's. Further, our survey-based measures capture self-reported experiences and may be subject to recall bias or under-reporting. That said, our results on prevalence and loss amounts broadly align with a 2022 study (Permanent TSB, 2024).

Table 1. Sample Validity (N=2,945)

	Population (2023)	Sample (N=2945)	Difference
Gender			
Male	49%	44%	5%
Female	51%	56%	5%
Age			
18–24	11%	4%	7%
25–34	17%	19%	2%
35–44	21%	26%	5%
45–54	18%	23%	5%
55–64	14%	15%	1%
65+	19%	13%	6%
Social Grade			
AB	12%	26%	14%
C1	34%	37%	3%
C2	20%	19%	1%
DE	28%	16%	12%
F	6%	2%	4%
Region			
Dublin	29%	28%	1%
Rest of Leinster	27%	27%	0%
Munster	27%	28%	1%
Ulster/Connacht	17%	17%	0%

Notes: Table reports mean proportions for the whole population and our sample. Population statistics for gender, age, and region are borrowed from the Central Statistics Office of Ireland (CSO), whereas statistics for social class are provided by the Association of Irish Market Research Organizations (AIMRO).

4 Methodology

4.1 Estimation Strategy

To investigate the relationship between fraud experience and our variables of interest, we estimate the following logit regression model.

$$FraudExperience_i = \beta_0 + \beta_1 X_i + \beta_2 Z_i + \varepsilon_i$$

where $FraudExperience_i$ denotes fraud experience for individual i. The outcome variable takes the value of one if the individual reports that they have experienced fraud and zero otherwise. β_0 is a constant term, X_i is a vector of socio-demographic control variables, and Z_i is a vector of behavioural and literacy variables. The socio-demographic controls in X_i include gender, age, education, income, and region. Education is a binary variable that takes the value of one if the respondent has attained a third-level education, and zero otherwise. Income is a binary variable that takes the value of one if annual household income is less than or equal to the sample median of €49,000, and zero oth-

erwise. Region is a binary variable that equals one if the individual resides in Dublin, and zero if the individual lives outside Dublin. The vector Z_i contains the variables of interest: financial literacy, fraud literacy, digital product use, financial product use, and risky online behaviour.[6] Each of our variables of interest is expressed in percentage terms ranging from 0 to 100.

Our estimation approach relies on running a sequence of models in which the explanatory variables of interest are added in separate stages. The specification presented above serves as the main specification. We estimate seven versions of this model, each of which adds a variable of interest from the vector Z_i. This choice allows us to examine the independent association of each variable of interest with fraud incidence, without confounding effects from including several potentially correlated variables. It also provides a clearer picture of which factors are most influential in isolation, before testing them jointly. This modelling strategy is consistent with approaches commonly used in applied work on financial vulnerability and fraud (Engels et al., 2021; Isaia et al., 2024). It balances interpretability with robustness: the intermediate models highlight the role of individual factors, while the full model captures their joint effect.

4.2 Descriptive Statistics

Table 2 reports summary statistics for a variety of demographics and financial variables in our data. Just over one in three individuals (35%) reported having experienced fraud. Among those who experienced fraud, the average number of incidents was 1.67, with a minority reporting as many as 16 cases. Although this upper bound highlights the extreme vulnerability of a small subset of respondents, the standard deviation of 1.50 indicates that such cases are relatively rare and that most individuals experienced only a small number of frauds.

In terms of socio-economic background, the sample leans toward lower-to-middle income households. 59% report annual household incomes of less than the sample median of €49,000. A strong educational profile emerges, with 69% having completed third-level education, leaving around one-third with lower qualifications.

[6] Detailed definitions of these variables of interest can be found in Table A3.

Table 2. Summary Statistics (N=2,945)

	Mean	SD	Min	Max
Victim of Fraud	0.35	0.48	0	1
No of Frauds Experienced	1.67	1.50	1	16
Male	0.44	0.49	0	1
Age 18-24	0.04	0.21	0	1
Age 25-34	0.19	0.39	0	1
Age 35-44	0.26	0.44	0	1
Age 45-54	0.23	0.42	0	1
Age 55-64	0.15	0.36	0	1
Age 65+	0.13	0.34	0	1
Third Level Education	0.69	0.46	0	1
Income < 49,000	0.59	0.49	0	1
Living in Dublin	0.28	0.45	0	1
Financial Literacy (%)	63.23	33.68	0	100
Fraud Literacy %	89.41	15.49	0	100
Digital Product Use %	54.88	18.51	0	100
Financial Product Use %	34.92	14.90	0	100
Risky Online Behaviour %	22.33	18.76	0	100

Notes: The number of observations is 2,945 for all variables except for 'Income', for which the number of observations is 2,717 because some respondents chose not to answer this question, and 'No of frauds experienced', which is only defined for the 35% (1,047) who said yes to experiencing fraud.

Financial literacy was measured through quiz-style questions on fundamental concepts such as interest rates, compounding, and inflation, with correct answers converted into percentage scores (Lusardi and Mitchell, 2014). Respondents scored an average of 63 out of 100, indicating a moderate grasp of these core financial principles. Fraud literacy was assessed through six scenario-based questions that tested respondents' ability to detect warning signs of scams and fraudulent offers (see Table A3 in appendix). Here, the average score was quite high at 89 out of 100, suggesting that many individuals are relatively good at recognising fraud when presented with hypothetical cases. Yet, despite this relatively strong fraud literacy, over one-third of respondents (35%) reported having experienced fraud in the past. This highlights the gap between recognising fraud in theory and avoiding it in practice, as scammers use techniques to exploit human behaviour such as instinctive rather than deliberative thinking.

For digital and financial product use, respondents were shown a list of digital and traditional financial products and asked whether they owned each one, with yes/no responses converted into percentage scores. On average, they reported owning 55% of the digital products compared with 35% of the traditional ones, highlighting the growing reliance on online platforms for everyday financial activity. At the same time, risky online behaviour was measured by asking respondents six questions to gauge how often they engage in practices such as clicking on suspicious links or oversharing personal information. The score ranges from 0 percent, indicating these respondents avoid all six

risky online behaviours, to 100 percent for the small minority demonstrating the riskiest online behaviours. Nonetheless, the average risky behaviour score of 23% shows that a sizeable minority of individuals admit to actions that could increase their vulnerability.

5 Fraud and Scam Incidence, Losses, Reporting & Recovery

A key contribution of our study lies in the detailed mapping of consumers' fraud experience in Ireland, which, to the best of our knowledge, has not been available in such an extensive and structured form before. While previous consumer surveys often highlight either prevalence rates or broad statistics on fraud, our data follow a clear sequence of questions. This allows us to capture not only whether individuals have experienced fraud, but also the consequences of these experiences, the extent of financial loss, the type of scams experienced, recovery outcomes, and reporting behaviour. This step-by-step approach provides a more comprehensive understanding of fraud exposure. It fills an important gap in the evidence base and offers insights that can complement industry based statistics and inform both policy and consumer protection measures.

5.1 Prevalence of Fraud and Scams

Figure 1 summarises the fraud experiences reported in our survey. From our sample of 2,945 respondents, just over a third (35%, or 1,047 individuals) reported experiencing some form of fraud or scam. This likely represents a lower bound for actual fraud experience as international studies suggest that many individuals do not admit to being victims of fraud (DeLiema et al., 2023). The individuals who reported experiencing fraud were impacted by 1.67 types of fraud on average. A minority reported as many as 16 types of fraud. Although this upper bound highlights the extreme vulnerability of a small subset of respondents, the standard deviation of 1.50 indicates that such cases are relatively rare and that most individuals experienced only a small number of frauds. Nearly two-thirds (63%) of those who reported experiencing fraud indicated that they had lost money as a result, while 37% reported no monetary loss. Reporting behaviour was also mixed: 62% of those who say they experienced fraud reported the incident to their bank, An Garda Síochána, or another supervisory authority, however, 38% did not. Taken together, these findings highlight both the scale of financial harm experienced by consumers and the challenges of reporting that remain central to the fraud landscape.

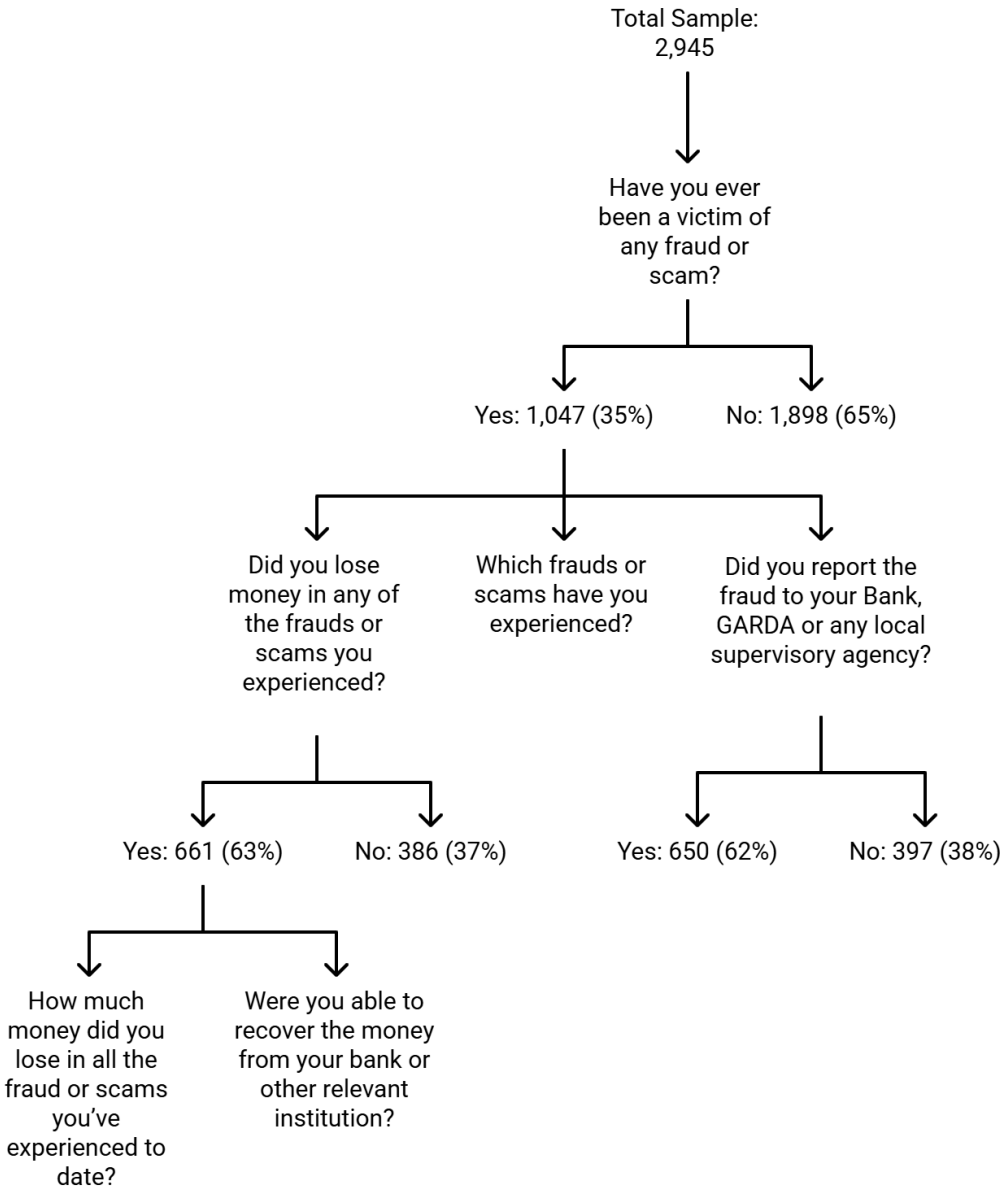

Figure 1. Fraud and Scam Incidence, Reporting & Recovery

Note: This flowchart summarizes the sample distribution across key stages of fraud incidence, reporting, and recovery. Percentages are calculated relative to the relevant subsample.

5.2 Types of Scams

While statistics collated from an industry perspective focus on high-level payment categories, such as credit transfers, our data allows us to delve further into the underlying nature of this fraud. Figure 2 shows the distribution of the types of fraud experienced by participants in our survey. This question was asked only to respondents who had previously indicated that they had experienced a fraud or a scam (N=1,047). Since this was a multiple-choice question, individuals could select more than one option, which is why the percentages sum to more than 100. The most commonly reported frauds were online purchase scams (48%) and debit or credit card fraud (34%). Other preva-

lent categories include fraud involving the impersonation of a delivery service (15%) and phishing or email scams (13%), both of which exploit trust in official communication channels. Less common, though still significant, were impersonation scams, investment scams, and PayPal-related frauds, each affecting between 6% and 7% of respondents.

A smaller share of respondents reported lottery or prize scams, accommodation fraud, and tech support scams (around 4–6% each). Less frequent but still present in the data are charity scams, romance scams, advance fee frauds, employment scams, invoice redirection, and travel or ticket frauds. Finally, 3% of respondents selected "other," which included scams such as crypto-related frauds, loans, and tax scams. These results highlight the diverse forms of fraud affecting consumers, with both everyday transactions and more specialised scams represented in the data.

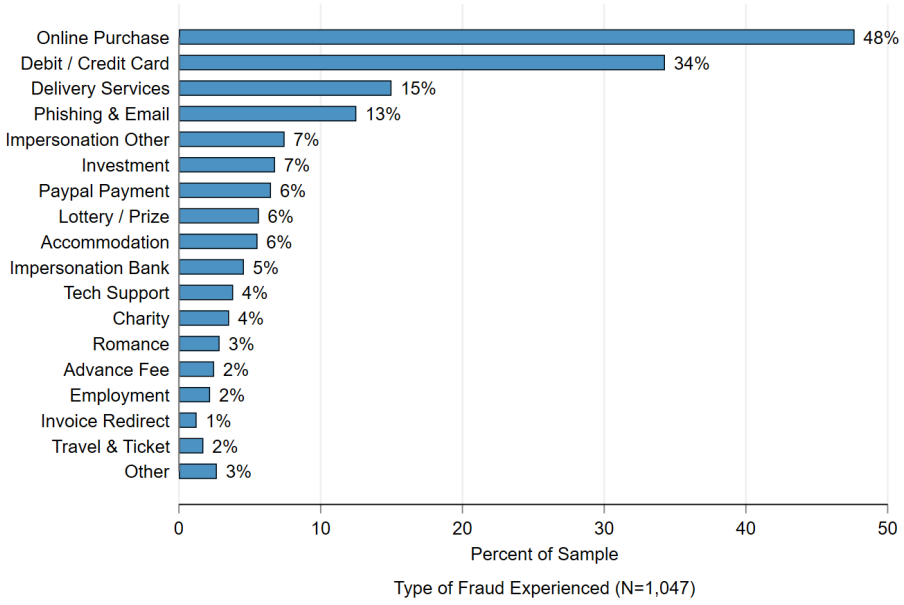

Figure 2. Type of Fraud Experienced

Note: Percentages are calculated from the subsample of respondents who reported experiencing at least one fraud or scam (N = 1,047). Multiple responses were possible, so totals exceed 100%.

5.3 Monetary losses

Figure 3 provides a breakdown of the amounts reported lost by those who experienced fraud or scams, complementing Figure 1. Among those who lost money, the majority reported relatively small amounts. Approximately 39% lost less than €249, while around 10% lost between €250 and €499. Only a small minority experienced losses above €1,000, with very few cases exceeding €10,000.

These results indicate that while substantial losses do occur, fraud more commonly involves smaller-scale financial harm affecting a large number of individuals. This aligns

with recent Irish and EU payment fraud data, suggesting fraudsters target high volume low value payments (CBI, 2025; EBA and ECB, 2024). Nonetheless, certain groups may experience monetary losses to a greater extent. This includes those with a lower education and who are experiencing above median financial difficulty (Figure 9 in the appendix). Almost 70% of those experiencing above the median level of financial difficulty reported having lost money to fraud compared to 60% for those below the median. This concurs with international evidence that over half of higher vulnerability consumers report falling for scams compared to a fifth of lower vulnerability consumers (Consumers International, 2025). Moreover, many victims suffer non-financial consequences (Brenner et al., 2020), all of which underscore the need for robust monitoring and preventive interventions.

Notably, 37% of those who reported experiencing fraud said they did not lose any money as a result of their fraud experience. There are two possible explanations for this "no money lost" category. Some cases may simply reflect unsuccessful scams that did not result in financial harm. In others, individuals may have reported promptly and recovered their funds, leading them to record no net loss. The latter interpretation appears more likely, given the relatively high reporting rate within this group (70%) and the fact that reporting and recovery are positively correlated (Pearson correlation coefficient, $r = 0.45$). This suggests that those who reported their experience of fraud were more likely to achieve recovery, and therefore may have viewed themselves as having not lost money.

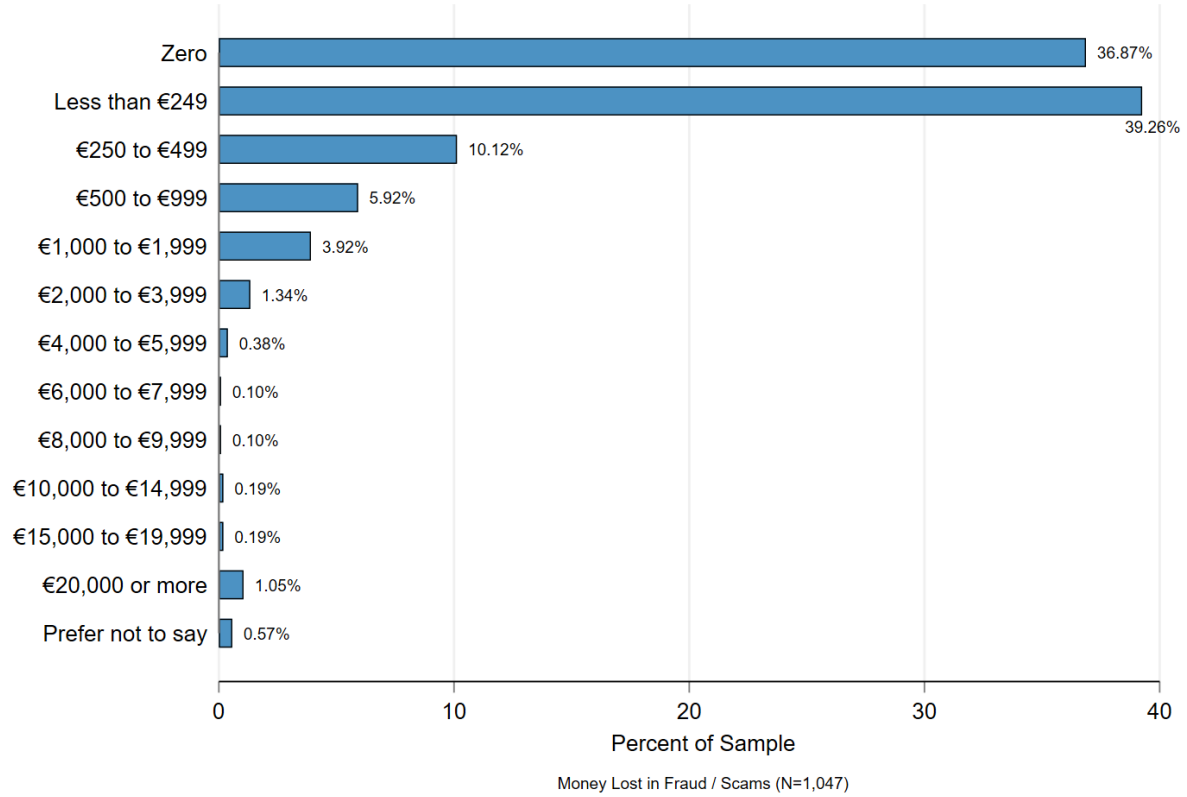

Figure 3. Monetary Losses from Fraud

Note: Percentages are based on respondents who reported experiencing at least one fraud or scam (N = 1,047). Reported amounts reflect self-reported total monetary losses across all incidents.

5.3.1 Linking the Type of Fraud & Monetary Losses

In this section, we examine how monetary losses vary across different types of fraud. Figure 2 on fraud types is based on a multiple-choice question, allowing respondents to report experiencing more than one type of fraud. By contrast, Figure 3 captures the total amount of money lost to fraud or scams overall, without distinguishing between specific types. As a result, monetary losses cannot be directly attributed to individual scams in the full sample. However, 70.58% of those who report experiencing fraud only reported being affected by a single type of fraud. For this subgroup, we can link losses to specific categories, as shown in Figure 4, which presents the distribution of monetary losses across common types of fraud in our data.

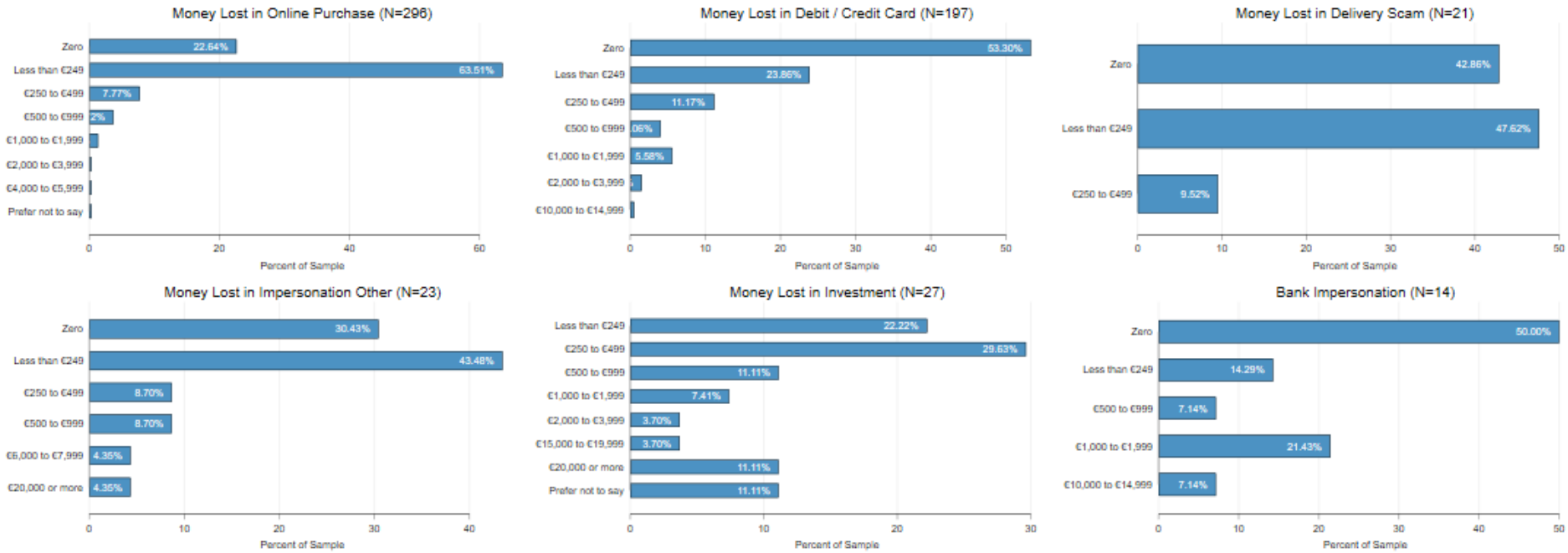

Figure 4. Linking Money Lost with Types of Fraud

Note: Each panel shows the distribution of self-reported monetary losses for respondents who experienced the specific fraud type indicated (sample sizes shown in panel titles). Percentages are calculated within each fraud category. The zeros represent those respondents who said they experienced fraud but did not lose money.

By far the vast majority of victims lost less than €250 for online purchase scams (86%), debit & credit card fraud (77%), delivery scams (91%) and other impersonation scams (74%). Among these categories between 23% and 53% did not lose any money at all. For example, in debit & credit card fraud, more than half of respondents reported zero losses. In online purchase scams, the most frequently reported scam type, over 20% of respondents did not lose money. Possible explanations include consumer scepticism, early reporting, interception and recovery. For bank impersonation fraud the small sample size warrants caution but suggests that 50% reported not losing any money. [7]

Investment fraud emerges as a clear outlier in our data. Although only 7% of respondents reported exposure to investment scams (Figure 2), almost none reported escaping without financial loss. This pattern suggests that engagement with investment scams almost invariably results in monetary harm, typically involving substantial amounts. Unlike unauthorised card fraud or online purchase scams, which can sometimes be reversed through chargebacks if reported swiftly, investment scams generally involve authorised fraud, and multiple voluntary transfers over a period of time, that are far more difficult to recover (UK Finance, 2025). Indeed, even in the UK where new reimbursement rules apply, recovery rates on investment scams were only about 50% in 2024 (UK Finance, 2025). Consequently, despite their relatively low prevalence, investment scams account for a disproportionate share of overall financial damage.[8]

The results in Figure 4 should be interpreted with caution. The analysis is limited to respondents who reported experiencing only a single type of fraud, allowing for a direct link between monetary losses and specific categories. This restriction substantially reduces sample sizes compared to the broader prevalence figures shown in Figure 2. As a result, the sample sizes in this figure are substantially smaller than the total number of individuals who reported each fraud type in Figure 2.[9] This restriction is necessary to provide a cleaner link between fraud type and money lost, but it comes at the cost of excluding individuals who were subject to multiple frauds. As such, the distributions presented here should be viewed as indicative patterns rather than precise estimates.

[7] For those who did lose money to bank impersonation fraud, similar to other impersonation fraud, losses tended to be for larger amounts than for debit card, delivery or online purchase fraud. Again due to the small sample size this result should be treated with caution.

[8] Data from a Garda press release, in October 2025, indicate that losses from investment fraud reached almost €31 million in Ireland in 2024 and almost €76 million in total between 2021 and end July 2025.

[9] For example, while roughly 503 out of 1,047 respondents reported experiencing an online purchase scam, the number falls to 296 in Figure 4 once cases involving multiple fraud types are excluded. Similarly, although approximately 356 individuals reported experiencing debit or credit card fraud, only 197 appear in this figure because it is limited to cases where card fraud was the sole scam reported.

5.4 Non-Reporting of Fraud to Authorities

Non-reporting of fraud remains a notable challenge. In our sample, 38% of those who admit to experiencing fraud did not report their experience to any authority.

The literature suggests several reasons for non-reporting. Victims may be unaware they have been defrauded, feel partly responsible, or experience embarrassment (Cross, 2015).[10] Others may consider the financial loss too small, view the incident as ambiguous, or be discouraged by the perceived attitudes of authorities and the complexity of reporting channels (Button et al., 2009). In addition, as Smith (2008) mentions, the sheer number of possible reporting avenues available, from family and friends to consumer bodies, the police or regulators can overwhelm victims. This can lead some individuals to avoid reporting altogether. Reporting of fraud may also vary among socio-demographic groups. In our sample reporting is lowest, at a third, among 18-24 year olds. Reporting increases with age to just over 70% among those aged 65 and over. It is slightly lower among females than males but the differences are small (see Figure 10 in the appendix).

Reporting also varies by the type of fraud. Restricting the sample to those who only experience one type of fraud, we observe that reporting rates are much higher on debit/credit card fraud and bank impersonation fraud. These reporting rates are over 90% compared to roughly 50% for online purchase and delivery scams and 40% for investment fraud. Again the same caveats apply to this restricted sample as for Figure 4 and the patterns should be viewed as indicative rather than precise.

5.5 The link between reporting and recovery

To capture the link between reporting and recovery, we asked respondents about these outcomes in sequence: first, whether they reported the fraud to any authority. Then, conditional on having lost money, whether they were able to recover their funds through their bank or another institution. Because only those who experienced monetary losses were asked about recovery, Figure 5 is based on the subsample of 661 respondents who answered both questions.[11] The results reveal a clear connection between reporting and recovery. Among those who did not report the fraud (left panel), only 13% managed to recover money, whereas recovery rates were substantially higher (57%) among those who reported (right panel). Our free text responses suggest that individuals who experienced fraud and say they did not report it but recovered funds, may include cases where bank detection systems identified and halted the fraud before the customer be-

[10] A recent Mastercard blog suggests that 59% of adults in a global poll say they would feel ashamed if they fell victim to an online scam, and about half would be embarrassed to tell anyone.

[11] There is a possibility that some individuals may have interpreted our question about losing money as net of recovery, in which case they would not have been asked whether they were able to recover their money. This means our estimates for recovery may represent a lower bound.

came aware of the issue. Nonetheless, the gap in recovery between those who report and those do not report is striking. It suggests that engagement with formal channels is associated with better financial outcomes after fraud.

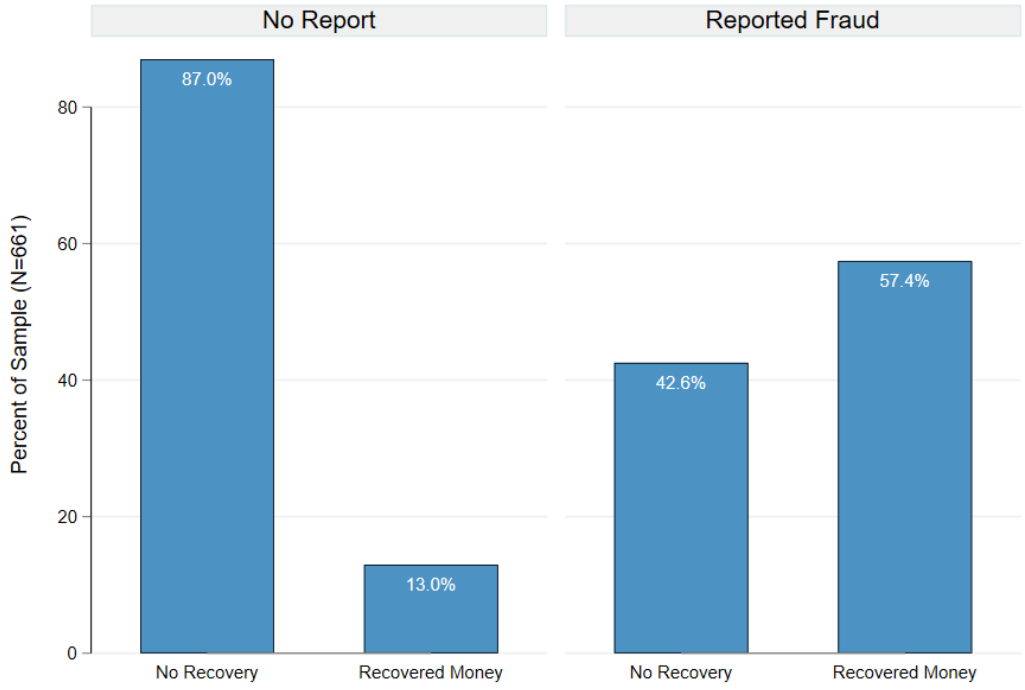

Figure 5. Linking Reporting & Recovery

Note: Bars display the proportion of respondents who reported recovering or not recovering money, conditional on whether they reported the fraud. Percentages are based on the subsample of respondents who lost money (N = 661).

Recovery is also linked with the type of fraud. The payment statistics for 2024 indicate that payment service users (i.e. customers) bear a higher share of the losses due to payment fraud on credit transfers (77%) and e-money payments (90%) than on card payments (13%) (CBI, 2025). To provide insights into recovery rates across underlying types of fraud, we again restrict our sample to individuals who report experiencing only one type of fraud. The same caveats apply as before. We observe significantly higher recovery rates for debit/credit card and bank impersonation fraud compared to all other types of fraud, conditional on reporting (See Figure 11 in the appendix). One likely explanation is that financial institutions often reimburse consumers for unauthorised fraud, unless the consumer has shown gross negligence (EBA, 2024).[12]

On the other hand, liability often falls on the consumer if they "authorise" the transaction (Praag and Jansen, 2025). This varies across payment types and jurisdictions (EBA, 2024). In the UK, new reimbursement rules became effective in October 2024. 88% of

[12] The EBA recommends further guidance to clarify the scope of gross negligence (EBA, 2024).

the money lost due to APP scams and covered by the new rules was returned to victims up to Q2 2025. Nonetheless, recovery rates remained lower for certain types of fraud such as CEO and investment fraud.[13]

Apart from reporting, another reason for not recovering funds could be late detection. A study by Alashwali et al. (2024) found that although notifications from banks or card issuers expedite detection, many victims only discover fraud by examining their statements themselves. This indicates that detection often occurs late. Survey evidence indicates that among young adults in Ireland, 20% report being unaware of fraud for over a year, while 30% took a week to notice (BPFI, 2019a). The growing sophistication of scams and the almost instant nature of payments makes any delay in reporting harder for financial institutions to intercept or recoup funds (Doig, 2016; Europol, 2025).[14]

Taken together, these findings underscore the need for effective campaigns to educate consumers about the association between reporting and recovery. Financial institutions should also make reporting processes simple to encourage those who experience fraud to report it. Forthcoming EU payment service regulations should assist with the earlier detection of fraudulent account activity (EPC, 2024). For instance, the proposals allow payment providers to swiftly share data across institutions. It also expands customer refund rights in certain situations such as bank impersonation fraud.

6 Predicting Fraud Experience

Table 3 reports the results from our regression analysis. Column (1) includes only the socio-demographic variables: gender, age, education, income, and Dublin residency. Gender is not a significant factor, suggesting that men and women are equally likely to experience fraud once other factors are taken into account. Age, however, shows a consistent pattern. Compared with the youngest group (18–24), all other age categories have a higher likelihood of experiencing fraud. Those aged 25–34 are around 13 percentage points more likely to experience fraud. Individuals aged 35–64 show probabilities of around 10 -15 percentage points higher. The oldest group (65+) also faces a higher risk, with a 13–14 percentage point increase in the likelihood of experiencing fraud relative to those aged 18-24. These findings contrast with studies from China,

[13] The UK reimbursement rules mean payment providers must reimburse victims of APP fraud for authorized payments up to £85,000 within 5 days, subject to certain restrictions including making a claim within 13 months of the payment. See PSR, PS24/7 Faster Payments APP scams reimbursement requirement: Confirming the maximum level of reimbursement requirements and PSR APP scams reimbursement dashboard for Q2 2025. Data from (UK Finance, 2025) indicate that reimbursement rates were highest for impersonation scams (just over 70%) and lowest for CEO scams (19%), with reimbursement rates of 68% for purchase scams and 50% for investment scams in 2024.

[14] For example, the EBA notes that fraud rates by value are about ten times higher, on average, for instant than conventional credit transfers (EBA, 2024).

Italy and Australia, which found that older individuals are less vulnerable to fraud (Wei et al., 2021; Isaia et al., 2024; Cross and Holt, 2025). One of the mechanisms thought to protect older adults despite their greater potential susceptibility to fraud is their limited online activity (Ross et al., 2014). Given the nature of our online panel, we may not fully capture older adults with limited online activity notwithstanding almost universal internet access (95%) among the wider population (CSO, 2025).

Examining the socio-economic indicators in Table 3, we observe that education, income, and location each contribute to shaping vulnerability to fraud.[15] Education is measured as a binary variable equal to one if the respondent has completed third-level education. Across all model specifications, individuals with higher education are significantly more likely to experience fraud. Average marginal effects range from 4.4 to 6.3 percentage points. In the fully specified model (Column 7), the effect is 5.2 percentage points. This finding contrasts with the common expectation that education should provide protection against fraudulent schemes (Engels et al., 2021; Wei et al., 2021). Instead, it suggests that individuals with higher education may be more financially active or digitally engaged, and therefore more exposed to fraud opportunities. This would also be consistent with the high share of online purchase fraud experienced in our sample.

Lower income individuals are between 3.6 and 8.1 percentage points more likely to experience fraud compared to higher-income individuals (€49,000+). This result highlights that financially vulnerable individuals face heightened risks. It is consistent with earlier research showing that economic strain can increase susceptibility to scams (Anderson, 2016). Finally, living in Dublin is also a significant predictor. Residents of the capital are about 3.7–4.6 percentage points more likely to experience fraud than those living elsewhere. This may reflect greater exposure due to a higher likelihood of younger, financially and digitally active individuals living in Dublin. It also echoes evidence that fraud risk is closely tied to situational exposure rather than demographic characteristics alone (Isaia et al., 2024).

Columns (2) and (3) introduce the literacy measures. Financial literacy, defined as knowledge of core concepts such as compounding and inflation, does not emerge as a significant factor. By contrast, each one percentage point increase in the fraud literacy score reduces the probability of experiencing fraud by 0.2 percentage points. While small in magnitude, this association is meaningful. For example, moving from a fraud literacy percentage score of 50% to 100% reduces the likelihood of experiencing fraud by 5 percentage points (-0.001 x 50). This finding resonates with recent work by (Xiao et al., 2022). They emphasise that being able to spot fraudulent cues is distinct from and more directly protective than general financial literacy. Importantly, much of the existing lit-

[15] We selected these variables based on the relevant theory but the use of a LASSO procedure selects the same set of variables.

erature has tended to emphasise financial literacy in broad terms, often treating it as the main proxy for consumer capability. Our results suggest that this approach may be too generic, as it overlooks the specific role of fraud literacy in shaping vulnerability to scams. Nevertheless, it is important to note that despite relatively high average fraud literacy scores (89.41%) in our sample, more than one-third of respondents reported experiencing fraud. This suggests that knowledge in principle is not always sufficient to prevent losses in practice (Table 2).

Finally, Columns (4), (5), and (6) incorporate financial product usage and risky online behaviour. Both digital and traditional product ownership increase the probability of experiencing fraud, each by about 0.4 percentage points for every additional product type owned. This implies that deeper engagement with the financial system, whether online or offline, broadens exposure to fraud risks. Risky online behaviour has the strongest effect. Each one percentage point increase raises the likelihood of experiencing fraud by 0.4 percentage points. Take for example, moving from a risky online behaviour score of 0 percent (i.e. no risky online behaviours) to 50 percent (i.e. reported engaging in 3 out of 6 risky online behaviours). This increases the likelihood of experiencing fraud from 0 percentage points to 20 percentage points (0.004 x 50). This result highlights that everyday online practices such as clicking on suspicious links or oversharing personal information are correlated with fraud vulnerability. This finding is in line with the Routine Activity Theory (Cohen and Felson, 2015), which argues that crime occurs when people are exposed to risks without enough protection or safeguards. Taken together, our results suggest that socio-demographic factors like age, education, and income matter. However, it is behavioural factors such as digital product use, financial product use, and especially risky online behaviour that consistently play the strongest role in predicting who experiences fraud.

Table 3. Logistic Regression predicting Fraud Experience (FV)

	(1) FV	(2) FV	(3) FV	(4) FV	(5) FV	(6) FV	(7) FV
Male	-0.010	-0.008	-0.010	-0.022	-0.018	-0.014	-0.023
	(0.019)	(0.020)	(0.019)	(0.019)	(0.019)	(0.019)	(0.020)
Age 25-34	0.127***	0.126***	0.130***	0.118***	0.106**	0.125***	0.114**
	(0.046)	(0.046)	(0.046)	(0.044)	(0.048)	(0.045)	(0.045)
Age 35-44	0.099**	0.099**	0.101**	0.101**	0.069	0.106**	0.095**
	(0.045)	(0.045)	(0.044)	(0.042)	(0.047)	(0.043)	(0.043)
Age 45-54	0.146***	0.146***	0.151***	0.157***	0.116**	0.169***	0.165***
	(0.045)	(0.045)	(0.045)	(0.044)	(0.047)	(0.044)	(0.044)
Age 55-64	0.092**	0.093**	0.098**	0.126***	0.072	0.132***	0.145***
	(0.047)	(0.047)	(0.046)	(0.045)	(0.049)	(0.046)	(0.047)
Age 65+	0.134***	0.135***	0.139***	0.187***	0.118**	0.185***	0.212***
	(0.048)	(0.048)	(0.047)	(0.047)	(0.050)	(0.048)	(0.049)
Third Level Education	0.056***	0.058***	0.063***	0.044**	0.044**	0.059***	0.052**
	(0.022)	(0.022)	(0.022)	(0.022)	(0.022)	(0.022)	(0.022)
Income <= 49,000	0.038*	0.037*	0.036*	0.056***	0.071***	0.058***	0.081***
	(0.020)	(0.020)	(0.020)	(0.020)	(0.021)	(0.020)	(0.021)
Dublin	0.046**	0.046**	0.044**	0.041**	0.044**	0.043**	0.037*
	(0.021)	(0.021)	(0.021)	(0.021)	(0.021)	(0.021)	(0.021)
Financial Literacy (%)		-0.000					-0.000
		(0.000)					(0.000)
Fraud Literacy (%)			-0.002**				-0.001*
			(0.001)				(0.001)
Digital Product Use (%)				0.004***			0.002***
				(0.001)			(0.001)
Financial Product Use (%)					0.004***		0.002***
					(0.001)		(0.001)
Risky Online Behavior (%)						0.004***	0.004***
						(0.001)	(0.001)
Observations	2,717	2,717	2,717	2,717	2,717	2,717	2,717

Notes: Logit average marginal effects, robust standard errors in parentheses. ***, **, and * indicate significance at 1, 5, and 10 percent critical levels. See Table A3 for variable definitions.

7 Robustness

Empirical results can be sensitive to modelling choices, variable definitions, and sample composition, making robustness analysis an essential component of credible empirical research. In this section, we assess the stability of our main findings by examining whether the estimated relationships between fraud experience and key behavioural and financial characteristics persist under alternative specifications and assumptions. In particular, we implement three complementary robustness checks.

First, we employ Specification Curve Analysis, which systematically estimates the effect of key variables across a wide range of plausible model specifications. This approach allows us to assess whether our conclusions depend on a narrow set of modelling decisions or instead reflect stable patterns that hold across alternative combinations of control variables. Second, we re-estimate the main regression model from Table A2 while augmenting the baseline specification with additional behavioural controls, including financial self-control and digital confidence. This exercise tests whether the estimated effects of fraud literacy and risky online behaviour are robust to the inclusion of related behavioural constructs that may capture overlapping dimensions of financial capability or digital engagement. Finally, to address potential concerns arising from differences between the sample composition and population benchmarks, we re-run the main analysis using population weights constructed from demographic characteristics. This weighted estimation allows us to verify that our results are not driven by over- or under-representation of particular groups in the survey sample, providing further reassurance that the findings are robust and generalisable.

7.1 Specification Curve Analysis

A common issue with regression analysis is that the estimated effect of a variable can change depending on which controls are included in the model. In Table A2, the coefficient on fraud literacy is negative and significant in some specifications, but becomes smaller and less precise when additional variables are added. Similarly, the effect of risky online behaviour is strong across models, but its magnitude may still depend on whether other behavioural measures, such as product use, are included simultaneously. This raises the concern that our conclusions may be influenced by the specific set of controls included in the model, rather than reflecting a stable underlying relationship. To deal with this, Simonsohn et al. (2020) proposes Specification Curve Analysis (SCA). Instead of focusing on a single preferred specification, SCA presents the results across a wide range of reasonable model choices, making it clear whether the main findings are robust or whether they depend on specific decisions regarding the controls included in the model. In this paper, we use SCA as a robustness check for two key behavioural

predictors, fraud literacy and risky online behaviour, since these variables play a central role in our analysis and could be most affected by alternative model specifications.

The specification curves in Figures 6 and 7 confirm that the key behavioural predictors remain robust across a wide range of control choices. In Figure 6, the fraud literacy score is consistently associated with a lower likelihood of fraud experience, with the majority of specifications producing negative coefficients. A large share of these estimates are statistically significant at the 95% level, including the main specification, which highlights that the protective effect of fraud literacy is not sensitive to the inclusion of different controls. Figure 7 shows that risky online behaviour is a strong and reliable predictor of fraud experience, with coefficients that are uniformly positive and statistically significant at the 95% level across every specification. This shows that the effect of risky online behaviour is stable regardless of the choice of controls. Taken together, the two specification curves show that fraud literacy consistently reduces, while risky online behaviour consistently increases, the probability of experiencing fraud, and that our findings are robust to alternative sets of controls.

7.2 Additional Controls & Sampling Weights

As a further robustness check, we assess whether our main results are sensitive to the inclusion of additional behavioural controls and to differences between sample and population compositions. First, Table A1 in the Appendix re-estimates the baseline specification from Table A2 while augmenting the model with additional behavioural variables, namely financial self-control and digital confidence. These variables capture related but distinct dimensions of consumers' financial and digital behaviour and provide a more stringent test of whether the estimated effects of fraud literacy and risky online behaviour are driven by omitted behavioural factors. The results remain highly stable: the direction, magnitude, and statistical significance of the key coefficients are largely unchanged relative to the baseline specification.

Second, Table A-2 re-estimates the main regression from Table A2 using population weights to adjust for discrepancies between the sample and population proportions across key demographic characteristics. This weighted analysis yields results that are very similar to the unweighted estimates in terms of coefficient size, statistical significance, and overall patterns of association. Taken together, these additional robustness checks provide strong reassurance that the main findings are not driven by omitted behavioural variables or by sample composition, and that the results are robust to alternative modelling choices and weighting schemes.

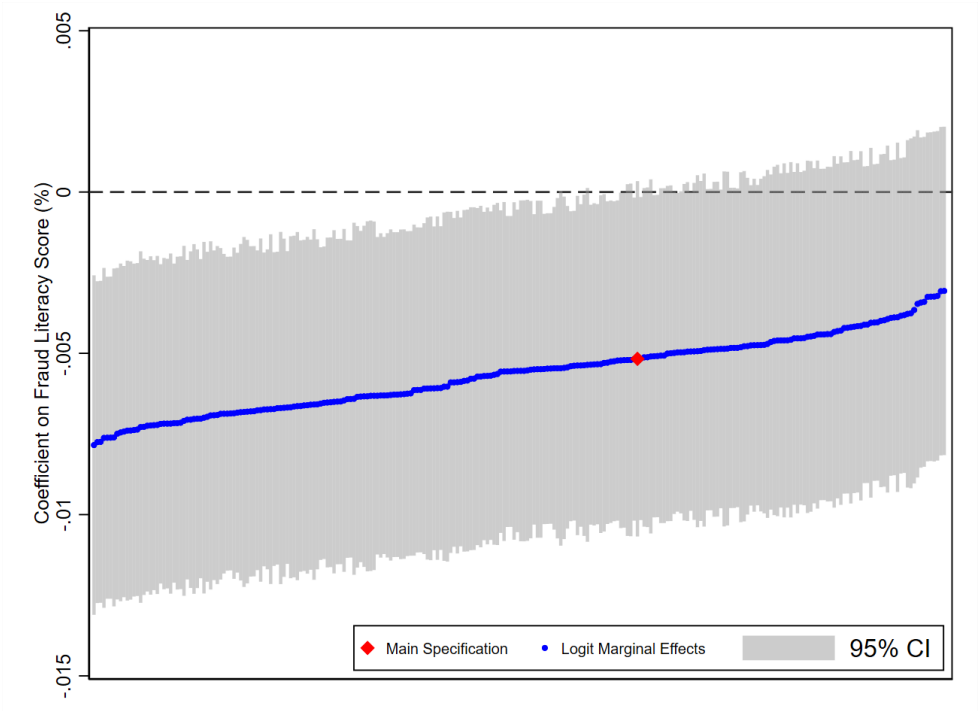

Figure 6. Specification Curve: Fraud Literacy Score

Note: Each point on the curve represents the estimated coefficient of the Fraud Literacy Score across alternative model specifications. The red diamond marks the main specification, while the shaded area shows the 95% confidence intervals.

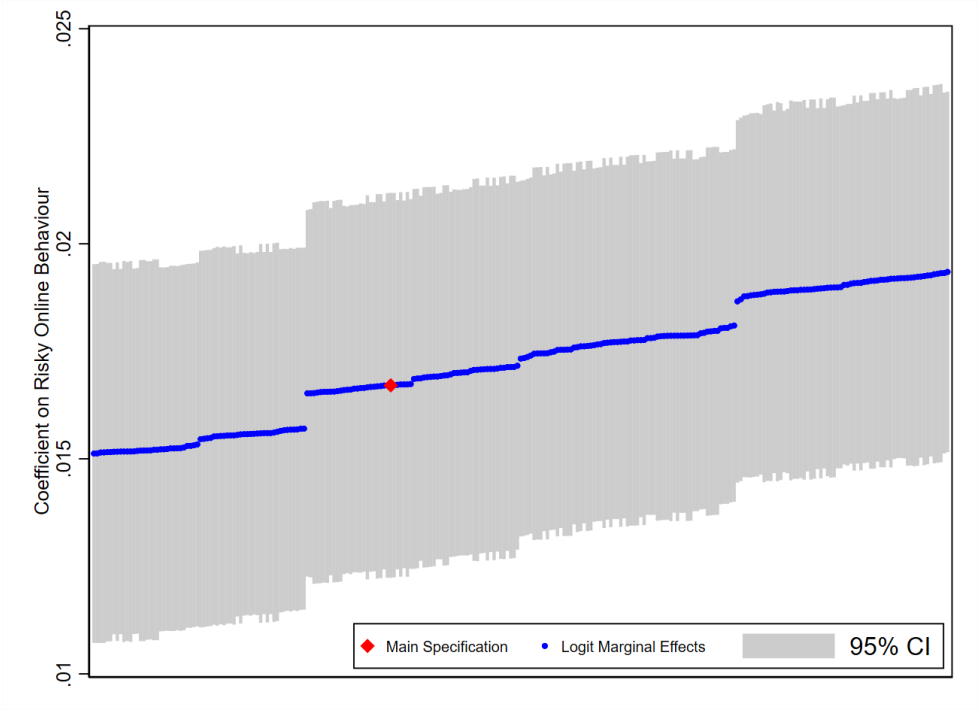

Figure 7. Specification Curve: Risky Online Behaviour

Note: Each point on the curve represents the estimated coefficient of Risky Online Behaviour across alternative model specifications. The red diamond marks the main specification, while the shaded area shows the 95% confidence intervals.

8 Conclusion & Discussion

In this paper, we examine individuals' experiences of fraud, monetary losses, reporting, and recovery. Our results show that more than one in three respondents reported experiencing fraud. Nearly two-thirds of these individuals incurred a financial loss. However, over a third of consumers do not report the incident, limiting their chances of recovery. Only 13% of those who lost funds but did not report the incident were able to recoup their losses, while 57% of those who reported the incident were able to do so.

A key contribution of this study is to move beyond descriptive prevalence figures and identify the behavioural and financial factors that correlate with consumer fraud experience. Our prediction analysis shows that socio-demographic variables such as age, income, and education explain some variation in fraud experience. However, behavioural factors are more predictive. Risky online behaviour emerges as the strongest behavioural predictor of fraud experience. Broader engagement with financial and digital products also increases predicted fraud experience. General financial literacy does not reduce predicted fraud experience. By contrast, fraud literacy, defined as the ability to identify fraudulent cues, is associated with a measurable, albeit modestly lower predicted exposure. These findings suggest that while financial education has long been a focus of consumer protection policies, more targeted approaches that address fraud-specific awareness and risky online practices may yield greater impact.

From a policy perspective, the evidence highlights the importance of combining consumer-focused and system-focused interventions. On the consumer side, interventions should prioritise practical fraud literacy, rather than relying solely on traditional financial literacy education. Enhancing consumer awareness of the need for reporting is also important. On the institutional side, strengthening detection mechanisms, simplifying reporting channels, and reviewing reimbursement guidelines remain critical to reducing both the incidence and consequences of fraud. The concentration of high monetary losses in investment fraud and the relatively low levels of recovery echo similar patterns in the UK, even with new reimbursement rules there. This further illustrates the importance of building consumer capabilities.

Finally, while the behavioural predictors examined here are powerful correlates of fraud experience, further research is needed to establish causal pathways and evaluate which interventions are most effective in practice.

References

Alashwali, E., Mysuru Chandrashekar, R., Lanyon, M., and Cranor, L. F. (2024). Detection and impact of debit/credit card fraud: Victims' experiences. *arXiv preprint*. Online: arXiv, accessed 26 August 2025.

Alliance, G. A.-S. and Feedzai (2024). Global state of scams report 2024.

Anderson, K. B. (2016). Mass-market consumer fraud: who is most susceptible to becoming a victim? *FTC Bureau of Economics*, (332).

B&A (2023). 23/52b ba consumer survey on nuisance communications.

Balakrishnan, V., Ahhmed, U., and Basheer, F. (2025). Personal, environmental and behavioral predictors associated with online fraud victimization among adults. *PLoS One*, 20(1):e0317232.

BPFI (2019a). Fraudsmart survey.

BPFI (2019b). older-irish-people-losing-almost-six-times-money-scammers-younger-generation-fraudsmart-survey.

BPFI (2024). Payment fraud report — h2 2023. Statistical report, Banking & Payments Federation Ireland.

BPFI (2025). Fraudsmart social engineering survey.

BPFI Core Research (2024). A measurement on online shopping and fraud.

Brenner, L., Meyll, T., Stolper, O., and Walter, A. (2020). Consumer fraud victimization and financial well-being. *Journal of Economic Psychology*, 76:102243.

Button, M., Lewis, C., and Tapley, J. (2009). Fraud typologies and the victims of fraud: Literature review.

Canadian Imperial Bank of Commerce (2025). Safe or scam: Test your knowledge of fraud with our quiz. https://us.cibc.com/en/privacy-security/banking-fraud/scam-quiz-personal.html.

CBI (2025). Payment fraud statistics. Technical report, Central Bank of Ireland.

Central Bank of Ireland (2025). Payment fraud statistics. https://www.centralbank.ie/statistics/data-and-analysis/payment-fraud-statistics.

Cohen, L. E. and Felson, M. (2015). Routine activity theory: A routine activity approach. In *Criminology theory*, pages 313–321. Routledge.

Competition and Consumer Protection Commission (2023). Financial wellbeing in ireland: Financial literacy and inclusion in 2023. Commissioned by the Competition and Consumer Protection Commission; Survey conducted by Ipsos MRBI using the OECD/INFE toolkit; 1,505 respondents.

Consumers International (2025). Building consumer resilience in digital finance.

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21(2):187–204.

Cross, C. and Holt, T. J. (2025). Does age matter? examining seniors' experiences of romance fraud. *Security Journal*, 38(1):46.

CSO (2025). Internet coverage and usage in ireland 2025.

DeLiema, M., Li, Y., and Mottola, G. (2023). Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type. *International Journal of Consumer Studies*, 47(3):1042–1059.

Deliema, M., Shadel, D., and Pak, K. (2020). Profiling victims of investment fraud: Mindsets and risky behaviors. *Journal of Consumer Research*, 46(5):904–914.

Doig, A. (2016). *Fraud: The counter fraud practitioner's handbook*. CRC Press.

EBA (2024). Opinion on new types of payment fraud and possible mitigations. Technical Report EBA-Op/2024/01, European Banking Authority (EBA).

EBA (2025a). Eba consumer trends report 2024/25. Technical Report EBA/REP/2025/08, European Banking Authority (EBA).

EBA (2025b). Risk assessment report of the european banking authority. Technical report, European Banking Authority (EBA).

EBA and ECB (2024). 2024 report on payment fraud. Technical Report EBA/ECB/2024, European Banking Authority; European Central Bank.

Engels, C., Kumar, K., and Philip, D. (2021). Financial literacy and fraud detection. In *Financial literacy and responsible Finance in the FinTech Era*, pages 124–146. Routledge.

EPC (2024). 2024 payment threats and fraud trends report. Technical Report EPC162-24/Version 1.0, European Payments Council (EPC).

Europol (2024). Internet organised crime threat assessment (iocta). Technical report, Publications Office of the European Union, Luxembourg.

Europol (2025). Europol, steal, deal and repeat - how cybercriminals trade and exploit your data – internet organised crime threat assessment. Technical report, Publications Office of the European Union, Luxembourg.

Federal Trade Commission (2025a). Consumer sentinel network data book 2024. Accessed: 2025-09-30.

Federal Trade Commission (2025b). New ftc data show big jump in reported losses to fraud: $12.5 billion in 2024. Accessed: 24 August 2025$.

Financial Conduct Authority (2024). Fraud, scams and financial promotions: Findings from the financial lives survey 2024. Consumer survey evidence on exposure to fraud, scams, and financial promotions in the UK.

Gurun, U. G., Stoffman, N., and Yonker, S. E. (2018). Trust busting: The effect of fraud on investor behavior. *The Review of Financial Studies*, 31(4):1341–1376.

Houtti, M., Roy, A., Gangula, V. N. R., and Walker, A. M. (2024). A survey of scam exposure, victimization, types, vectors, and reporting in 12 countries. arxiv. *arXiv preprint arXiv:2407.12896*.

Isaia, E., Oggero, N., and Sandretto, D. (2024). Is financial literacy a protection tool from online fraud in the digital era? *Journal of Behavioral and Experimental Finance*, 44:100977.

Koning, L., Junger, M., and Veldkamp, B. (2024). Risk factors for fraud victimization: The role of socio-demographics, personality, mental, general, and cognitive health, activities, and fraud knowledge. *International review of victimology*, 30(3):443–479.

Lokanan, M. E. and Liu, S. (2021). The demographic profile of victims of investment fraud: an update. *Journal of Financial Crime*, 28(3):647–658.

Lourie, B., Nekrasov, A., Truong, P., and Zhu, C. (2023). Crypto fraud and investing behavior. *Available at SSRN 4650849*.

Lusardi, A. and Mitchell, O. S. (2014). The economic importance of financial literacy: Theory and evidence. *American Economic Journal: Journal of Economic Literature*, 52(1):5–44.

OECD (2026). Consumer finance risk monitor 2026. Technical report, OECD Publishing, Paris, France.

Permanent TSB (2024). Reflecting ireland: Managing our money in a digital world (q2 2024). Quarterly research report, Permanent TSB.

Pew Research Center (2025). Online scams and attacks in america today. Nationally representative survey evidence on U.S. adults' exposure to online scams and fraud attempts.

Praag and Jansen (2025). Forthcoming european regulation: Who bears liability in cases of online payment fraud? Accessed 26 August 2025.

Ross, M., Grossmann, I., and Schryer, E. (2014). Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. *Perspectives on Psychological Science*, 9(4):427–442.

Simonsohn, U., Simmons, J. P., and Nelson, L. D. (2020). Specification curve: Descriptive and inferential statistics on all reasonable specifications. *American Economic Review*, 110(11):3645–83.

Smith, R. G. (2008). Coordinating individual and organisational responses to fraud. *Crime, law and social change*, 49(5):379–396.

UK Finance (2025). Annual fraud report 2025. Accessed: 2025-09-30.

Varadarajan, S. (2025). Insights from irish payment fraud statistics. Technical report, Central Bank of Ireland. Statistical Publication; includes fraud types, rates by payment method, cross-border trends, SCA data.

Wei, L., Peng, M., and Wu, W. (2021). Financial literacy and fraud detection——evidence from china. *International Review of Economics & Finance*, 76:478–494.

Wise (2024). Wise consumer scam survey.

Xiao, X., Li, X., and Zhou, Y. (2022). Financial literacy overconfidence and investment fraud victimization. *Economics Letters*, 212:110308.

Appendix

8.1 Choice of Variables

Figure 8 presents a correlation matrix of our explanatory variables, where the strength and direction of pairwise associations are displayed numerically. Positive correlations are shaded in green. Negative correlations are shaded in red. Larger absolute values indicate stronger relationships between variables. Smaller values reflect weaker associations. Most correlations are relatively modest, suggesting that each variable captures a distinct underlying dimension of financial behaviour or knowledge. The strongest association appears between digital product use and digital confidence (r = 0.47). This is intuitive given that individuals who own and use more digital products are also likely to report higher confidence in using them. Digital product use is also moderately correlated with financial product use (r = 0.39). This reflects the complementarity between traditional and digital financial engagement. Fraud literacy is positively associated with financial literacy (r = 0.32), but the correlation is far from perfect. This indicates that general financial knowledge and the ability to detect fraud represent related but distinct competencies.

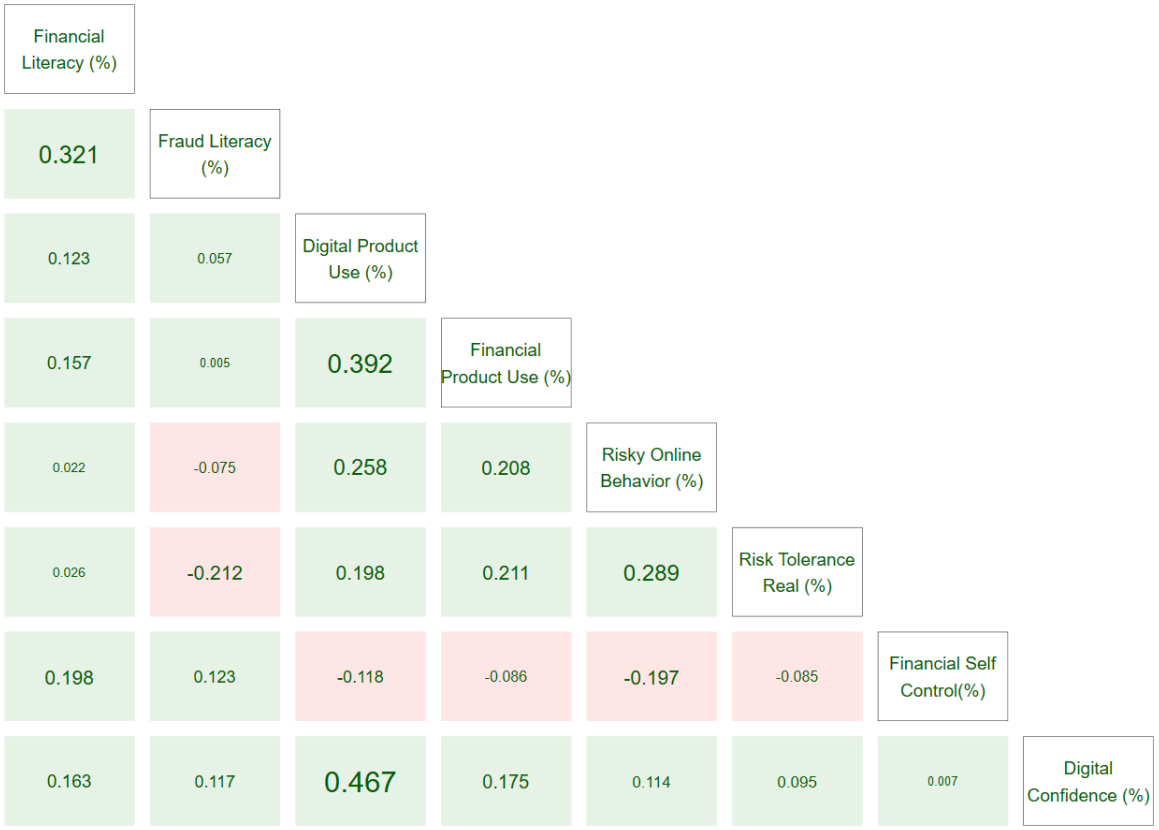

Figure 8. Pairwise Correlations between Explanatory Variables

Note: This figure presents pairwise Pearson correlation coefficients between the explanatory variables used in the analysis. Green cells indicate positive correlations and red cells indicate negative correlations. The size of the text reflects stronger correlations in absolute terms. All correlations are based on the full survey sample (N = 2,945).

Other correlations, such as those involving risky online behaviour, financial self-control, and risk tolerance, remain below 0.30. This provides reassurance that these variables do not exhibit problematic overlap. Indeed, the low to moderate levels of correlation across the table indicate that multicollinearity is unlikely to pose a major concern in our regression analysis. While multicollinearity does not appear to be a major concern, we adopt a parsimonious modelling strategy. We focus on the predictors most directly linked to fraud incidence in theory (i.e. fraud literacy and risky online behaviour) and prior literature (i.e. financial literacy and digital product use). Other behavioural constructs, such as risk tolerance, digital confidence, and financial self-control, are treated as supplementary measures. Including them in robustness checks confirms that they do not alter the main findings. This supports our decision to exclude them from the baseline specification in the interest of clarity and interpretability.

8.2 Variable Definitions

Table A3. Variable Definitions

Variable	Definition
Financial Literacy (%)	Percentage score based on number of correct answers to the following four questions. 1. Imagine that you have to wait for one year to receive a lottery prize worth €1,000 and inflation stays at 2%. In one year's time how much will they be able to buy with your prize money? (a) More than today (b) Exactly the same (c) Less than today (d) It depends on the types of things that they want to buy (e) Don't know
Continued on next page	

Table A3 – continued from previous page

Variable	Definition
	2. Imagine that someone puts €100 into a no fee, tax-free savings account with a guaranteed interest rate of 2% per year. They don't make any further payments into this account and they don't withdraw any money. How much would be in the account at the end of the first year, once the interest payment is made? Enter '555' if 'Don't Know'. Correct Answer:€102 3. Imagine an investment that had a 15% return in the first month, an 8% loss in the second month and a 5% return in the third month. Is this investment considered volatile? (a) Yes (b) No (c) Depends on the investment type (d) Don't know

Continued on next page

Table A3 – continued from previous page

Variable	Definition
	4. Imagine that someone puts €100 into a no fee, tax free savings account with a guaranteed interest rate of 2% per year. They don't make any further payments into this account and they don't withdraw any money. How much would be in the account at the end of FIVE years, after the final compound interest payment is made? (a) More than €110 (b) Exactly €110 (c) Less than €110 (d) Impossible to tell from the information given (e) Don't Know

Continued on next page

Table A3 – continued from previous page

Variable	Definition
Fraud Literacy (%) (Canadian Imperial Bank of Commerce, 2025)	Percentage score based on number of correct answers to the following four questions. In this section, each scenario we present outlines a situation where you may encounter potential risks or fraudulent activities. Your task is to select the most appropriate response from the provided options. Please read each scenario carefully before answering. 1. You met someone on a dating site a few months ago. Even though they live abroad, there was an immediate connection and they told you they love you almost immediately. One day, they message you upset: a family member you hadn't heard of is in the hospital. They're stressed because they can't pay the medical bills, and ask if you can send some money to help. How would you respond in this situation? (a) Get their bank details and send a wire transfer immediately (b) Ask more questions about the sick family member (c) Don't send any money and stop communicating

Continued on next page

Table A3 – continued from previous page

Variable	Definition
	2. You come across an online ad to invest in a start-up. The company has a limited time, risk-free offer that lets you withdraw funds from your locked-in retirement savings to invest in shares. You're promised high dividends and your entire investment back without paying fees or tax. Since you know you'll be taxed when you make a withdrawal, this seems too good to be true. This is a scam. How can you tell? (a) It's marketed to people with retirement savings. (b) You found this opportunity online. (c) You're promised high dividends without paying fees or tax 3. After months of job hunting, you receive an email from a recruitment agency about a job opportunity. Here's how it reads: (Participants are shown a screenshot from an email which describes that the job pays €5000 monthly working from home, but requires a €200 training deposit and requests for card details for the transfer). How would you respond in this situation? (a) Reply to the email and ask for more details (b) Send them your credit card information (c) Don't reply to this email and ignore it

Continued on next page

Table A3 – continued from previous page

Variable	Definition
	4. You're shopping for a new TV, and you find a classified ad online selling the TV you wanted at a discounted price. The ad states you can get the TV overnight with free delivery, but the seller only accepts payments via wire transfer. The site indicates there's only one unit left. Not wanting to miss the opportunity, you send a wire transfer. Once the transfer is completed, the TV never arrives. Why was this a scam? (a) You saw the product in an online ad. (b) The seller promised free delivery for the TV. (c) You're asked to pay through wire transfer. 5. You get a message from an unknown number. The person on the other end claims to be your grandchild and is in distress. You have the following conversation: (Participants are shown a screenshot from a message conversation where the sender pretends to be the grandchild and asks to send a wire transfer to repair the car that was involved in an accident.) How would you respond in this situation? (a) Offer to send them an e-Transfer instead. (b) Contact them directly at the number you have for them. (c) Ask for their account details to send a wire transfer.

Continued on next page

Table A3 – continued from previous page

Variable	Definition
	6. You post an ad to sell your couch on an online marketplace. Later, you receive an email from someone interested in buying your couch. They ask if they can send you a cheque for the item and you agree. But when you get the cheque, it's written for more than your selling price. You let the buyer know and they tell you the extra funds are to cover shipping costs for a third-party, and you need to send the extra amount to the shipper. How would you respond in this situation? (a) Deposit the cheque and transfer the money. (b) Send the couch to them before the cheque clears. (c) Ask for a cheque with the correct amount and make sure it clears.
Digital Product Use (%)	Percentage score based on the number of digital financial products from the following that the participant currently uses, either alone or jointly: Internet Banking (e.g. AIB, BOI 365 online); Mobile Banking Apps; P2P / Fintech Services (e.g. Revolut, Wise, N26, Circle Pay); Digital Wallets (e.g. Apple Pay, Google Pay); Online Payment Services (e.g. PayPal, Stripe); Buy Now Pay Later Services (e.g. Klarna, Humm, Revolut Pay Later); Crypto Asset Exchanges and Wallets (e.g. Coinbase, Binance, Bitcove); Investment and Trading Platforms (for Stocks or Forex)

Continued on next page

Table A3 – continued from previous page

Variable	Definition
Financial Product Use (%)	Percentage score based on the number of financial products from the following that the participant currently uses, either alone or jointly: Current account with a bank or building society for personal use, excluding business accounts; Credit card; Savings account; Car loan; Personal loan; Mortgage; Overdraft; Investments (eg: stocks, shares); Crypto assets; Loan from a licensed moneylender; In store credit.
Risky Online Behaviour (%) (developed by the authors based on common fraud exposure mechanisms)	Percentage score calculated based on participants' response to the following questions, where the responses were coded as 1 for "Yes" and 0 for "No". 1. Have you made online purchases from new or unfamiliar websites in the last 6 months? 2. Do you frequently respond to unsolicited messages offering discounts or promotions? 3. Have you ever shared your banking or debit/credit card details via email, phone or messaging apps? 4. Have you ever sent money to someone you met online but have never met in person? 5. Do you use multi-factor authentication (eg, SMS code, email verification) for online payments? 6. Do you frequently make high-value purchases online (e.g. over €500)?

Continued on next page

Table A3 – continued from previous page

Variable	Definition
Risk Tolerance Real (%)	Percentage score based on responses to the following questions, where the participant indicates their likelihood to engage in the described behaviour on a scale 1 to 7, where 1 represents "Extremely Unlikely" and 7 represents "Extremely Likely". The higher the score, the higher the respondent's risk tolerance. 1. Investing 10% of your annual income in a moderate growth mutual fund. 2. Betting a day's income at a high-stake poker game. 3. Investing 5% of your annual income in a very speculative stock. 4. Investing 10% of your annual income in a new business venture.
Financial Self Control(%)	Percentage score based on the responses "Yes" (coded as 0) or "No" (coded as 1) to the following questions related to financial self-control, where the lower the score, the higher the level of financial self-control. Please reflect on your usual behaviour and select the response that best represents how often you engage in the described actions. 1. I usually spend more than I planned to when I go shopping. 2. If I see something I want, I usually buy it immediately, even if it wasn't planned 3. I often buy things without considering whether I can afford them. 4. I carefully consider whether I need something before buying it (reverse coded). 5. I keep track of my spending to make sure I stay within my budget (reverse coded). 6. I find it hard to follow through with financial goals I set for myself.

Continued on next page

Table A3 – continued from previous page

Variable	Definition
Digital Confidence (%)	Percentage score based on responses to the following questions, where the participant indicates their likelihood to engage in the described behaviour on a scale 1 to 7, where 1 represents 'Not at all Confident' and 7 represents 'Very Confident'. The higher the score, the higher the respondent's confidence. 1. Transferring money 2. Paying with a mobile device (e.g. mobile phone or tablet) instead of using cash 3. Ensuring the safety of sensitive information when making an electronic payment or using online banking

8.3 Supplementary Figures

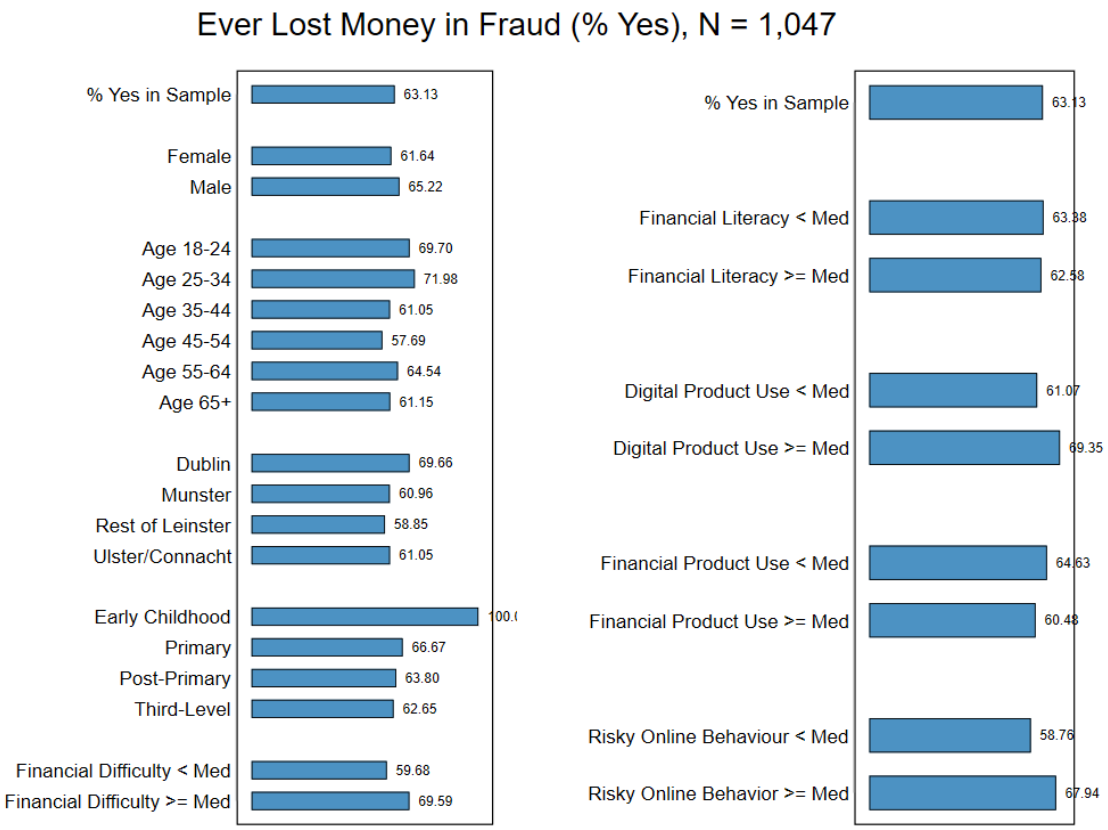

Figure 9. Ever Lost Money in Fraud by demographic and financial characteristics

Note: This figure reports the percentage of respondents who reported losing money as a result of fraud, conditional on having experienced at least one fraud or scam. The outcome variable is therefore defined only for individuals who answered "yes" to having ever been a victim of fraud (N = 1,047). This corresponds to 35% of the full survey sample. Percentages are shown separately by demographic and financial characteristics. Bars indicate the share within each subgroup who reported a monetary loss. Financial and behavioural variables are split at the sample median. All percentages are calculated within the relevant subsample. The figure is based on those who report losing money before any recoveries.

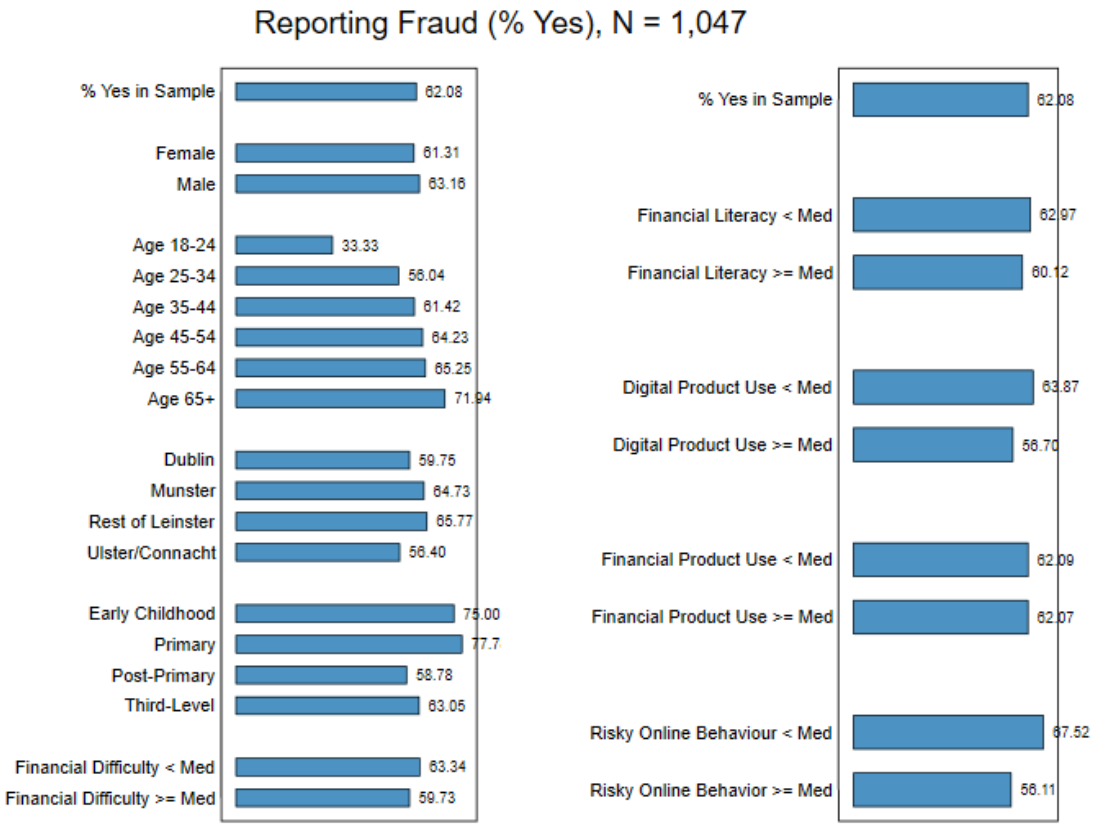

Figure 10. Fraud reporting by demographic and financial characteristics

Note: This figure reports the percentage of respondents who reported the fraud to a bank, An Garda Síochána, or another relevant authority, conditional on having experienced at least one fraud or scam. The reporting outcome is therefore defined only for individuals who answered "yes" to having ever been a victim of fraud (N = 1,047). This corresponds to 35% of the full survey sample. Percentages are shown by demographic and financial characteristics. Bars indicate the share within each subgroup who reported the incident. Financial and behavioural variables are split at the sample median. All percentages are calculated within the relevant subsample.

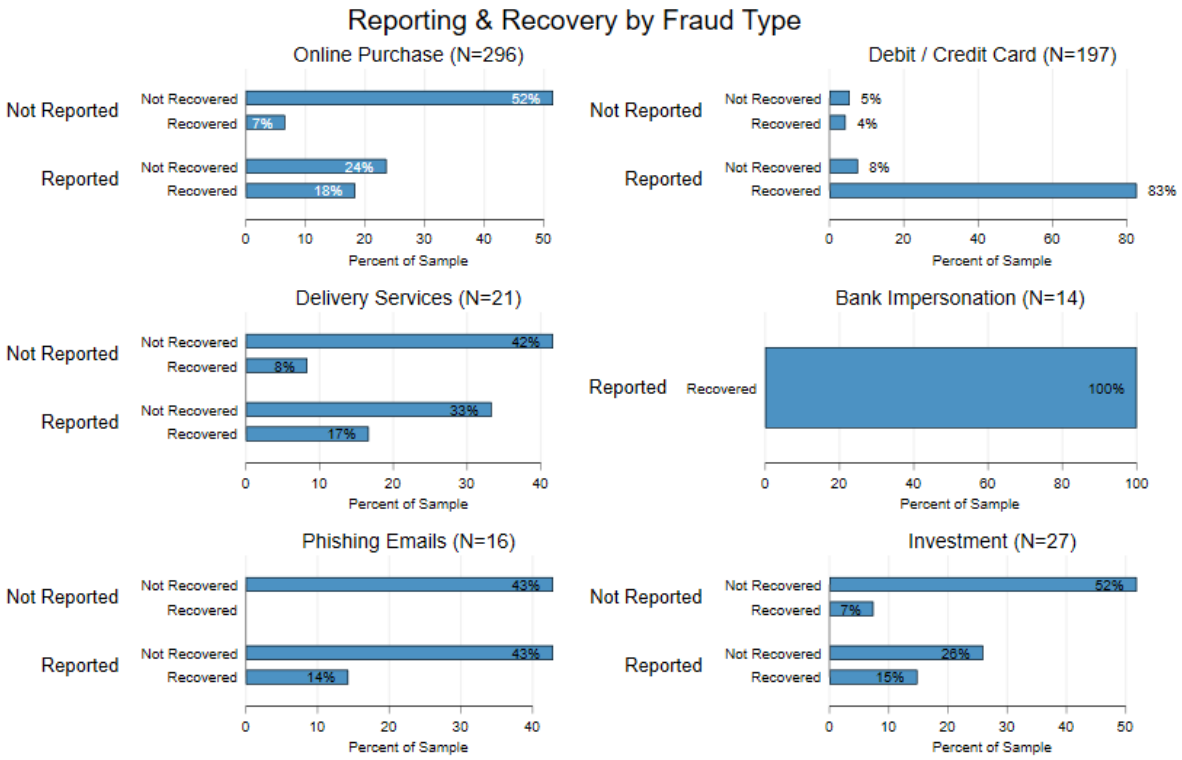

Figure 11. Reporting and Recovery by Fraud Type

Note: This figure examines the relationship between fraud reporting and monetary recovery by fraud type. The sample is restricted to respondents who reported experiencing only one type of fraud, allowing recovery outcomes to be directly linked to a specific fraud category. The figure focuses on the six most prevalent fraud types in the data, with sample sizes shown in panel titles. For each fraud type, respondents are first grouped by whether they reported the fraud to a bank, An Garda Síochána, or another relevant authority versus if they recovered the money lost or not. Percentages are calculated within fraud-type–specific subsamples. The figure is intended to illustrate how reporting behaviour is associated with recovery outcomes across different types of fraud.

8.4 Robustness Checks

Table A1. Robustness Check: Additional Controls

VARIABLES	(1) FV	(2) FV	(3) FV	(4) FV	(5) FV	(6) FV	(7) FV	(8) FV	(9) FV	(10) FV
Male	-0.010	-0.008	-0.010	-0.022	-0.018	-0.014	-0.021	-0.001	-0.012	-0.018
	(0.019)	(0.020)	(0.019)	(0.019)	(0.019)	(0.019)	(0.020)	(0.019)	(0.019)	(0.021)
Age 25-34	0.127***	0.126***	0.130***	0.118***	0.106**	0.125***	0.127***	0.120***	0.126***	0.113**
	(0.046)	(0.046)	(0.046)	(0.044)	(0.048)	(0.045)	(0.045)	(0.046)	(0.046)	(0.045)
Age 35-44	0.099**	0.099**	0.101**	0.101**	0.069	0.106**	0.103**	0.093**	0.100**	0.092**
	(0.045)	(0.045)	(0.044)	(0.042)	(0.047)	(0.043)	(0.043)	(0.044)	(0.044)	(0.043)
Age 45-54	0.146***	0.146***	0.151***	0.157***	0.116**	0.169***	0.155***	0.142***	0.149***	0.160***
	(0.045)	(0.045)	(0.045)	(0.044)	(0.047)	(0.044)	(0.044)	(0.045)	(0.045)	(0.045)
Age 55-64	0.092**	0.093**	0.098**	0.126***	0.072	0.132***	0.108**	0.098**	0.096**	0.144***
	(0.047)	(0.047)	(0.046)	(0.045)	(0.049)	(0.046)	(0.046)	(0.046)	(0.047)	(0.047)
Age 65+	0.134***	0.135***	0.139***	0.187***	0.118**	0.185***	0.157***	0.144***	0.140***	0.210***
	(0.048)	(0.048)	(0.047)	(0.047)	(0.050)	(0.048)	(0.047)	(0.048)	(0.048)	(0.049)
Third Level Education	0.056***	0.058***	0.063***	0.044**	0.044**	0.059***	0.053**	0.065***	0.053**	0.057**
	(0.022)	(0.022)	(0.022)	(0.022)	(0.022)	(0.022)	(0.022)	(0.022)	(0.022)	(0.023)
Income <= 49,000	0.038*	0.037*	0.036*	0.056***	0.071***	0.058***	0.043**	0.034*	0.041**	0.078***
	(0.020)	(0.020)	(0.020)	(0.020)	(0.021)	(0.020)	(0.020)	(0.020)	(0.020)	(0.021)
Dublin	0.046**	0.046**	0.044**	0.041**	0.044**	0.043**	0.044**	0.049**	0.046**	0.039*
	(0.021)	(0.021)	(0.021)	(0.021)	(0.021)	(0.021)	(0.021)	(0.021)	(0.021)	(0.021)
Financial Literacy (%)		-0.000								-0.000
		(0.000)								(0.000)
Fraud Literacy (%)			-0.002**							-0.001
			(0.001)							(0.001)
Digital Product Use (%)				0.004***						0.003***
				(0.001)						(0.001)
Financial Product Use (%)					0.004***					0.002***
					(0.001)					(0.001)
Risky Online Behavior (%)						0.004***				0.004***
						(0.001)				(0.001)
Risk Tolerance Real (%)							0.002***			-0.000
							(0.001)			(0.001)
Financial Self Control(%)								-0.001***		-0.001*
								(0.000)		(0.000)
Digital Confidence (%)									0.001	-0.001
									(0.001)	(0.001)
Observations	2,717	2,717	2,717	2,717	2,717	2,717	2,717	2,717	2,717	2,717

Notes: This table reports logit average marginal effects from regressions predicting fraud experience (FV). Robust standard errors are shown in parentheses. All specifications include the baseline set of socio-demographic controls: gender, age group, third-level education, income (€49,000), and Dublin residence. Columns extend the baseline model by sequentially adding behavioural and financial variables. In addition to the variables included in Table 3, selected specifications incorporate financial self-control and digital confidence as additional controls to test whether the estimated effects of fraud literacy and risky online behaviour are robust to related behavioural constructs. All behavioural and literacy variables are expressed in percentage terms (0–100). The number of observations is 2,717 in all specifications. ***, **, and * denote statistical significance at the 1%, 5%, and 10% levels, respectively. See Table A3 for variable definitions.

Table A2. Robustness Check: Sampling Weights

VARIABLES	(1) FV	(2) FV	(3) FV	(4) FV	(5) FV	(6) FV	(7) FV
Male	0.006	0.006	0.006	-0.008	-0.005	0.001	-0.012
	(0.023)	(0.024)	(0.024)	(0.024)	(0.024)	(0.024)	(0.025)
Age 25-34	0.078	0.078	0.082	0.072	0.052	0.077	0.066
	(0.056)	(0.056)	(0.057)	(0.052)	(0.059)	(0.057)	(0.056)
Age 35-44	0.045	0.045	0.047	0.054	0.012	0.053	0.047
	(0.054)	(0.054)	(0.054)	(0.050)	(0.057)	(0.055)	(0.054)
Age 45-54	0.108*	0.108**	0.113**	0.129**	0.073	0.129**	0.130**
	(0.055)	(0.055)	(0.055)	(0.051)	(0.058)	(0.056)	(0.056)
Age 55-64	0.072	0.072	0.076	0.119**	0.048	0.111*	0.132**
	(0.056)	(0.056)	(0.057)	(0.053)	(0.059)	(0.059)	(0.058)
Age 65+	0.081	0.082	0.086	0.158***	0.057	0.129**	0.171***
	(0.058)	(0.058)	(0.058)	(0.055)	(0.060)	(0.060)	(0.060)
Third Level Education	0.101***	0.102***	0.107***	0.090***	0.088***	0.103***	0.093***
	(0.026)	(0.027)	(0.026)	(0.026)	(0.026)	(0.026)	(0.028)
Income <= 49,000	0.036	0.036	0.034	0.059**	0.074***	0.054**	0.084***
	(0.024)	(0.024)	(0.024)	(0.024)	(0.024)	(0.024)	(0.025)
Dublin	0.055**	0.055**	0.053**	0.045*	0.052**	0.053**	0.042*
	(0.025)	(0.025)	(0.025)	(0.025)	(0.025)	(0.025)	(0.025)
Financial Literacy (%)		-0.000					-0.000
		(0.000)					(0.000)
Fraud Literacy (%)			-0.001*				-0.001
			(0.001)				(0.001)
Digital Product Use (%)				0.004***			0.003***
				(0.001)			(0.001)
Financial Product Use (%)					0.005***		0.002***
					(0.001)		(0.001)
Risky Online Behavior (%)						0.004***	0.003***
						(0.001)	(0.001)
Observations	2,717	2,717	2,717	2,717	2,717	2,717	2,717

Notes: This table reports logit average marginal effects from regressions predicting fraud experience (FV), re-estimated using population sampling weights to adjust for differences between sample and population proportions across key demographic characteristics. Robust standard errors are shown in parentheses. All specifications mirror those in Table 3, with the same set of socio-demographic controls—gender, age group, third-level education, income (€49,000), and Dublin residence—and sequential inclusion of behavioural and literacy variables. All behavioural and literacy measures are expressed in percentage terms (0–100). The number of observations is 2,717 in all specifications. ***, **, and * denote statistical significance at the 1%, 5%, and 10% levels, respectively. See Table A3 for variable definitions.

T: +353 (0)1 224 6000
www.centralbank.ie
publications@centralbank.ie

Bosca PO 559, Baile Átha Cliath 1, Éire
PO Box 559, Dublin 1, Ireland