Fraud Prevention Education for Older Adults: A Business Case for Financial Institutions

Daniel Chinaemerem[1], Oguntuase Michael[1',2,] Eziefule Chinonso[2], Mayegun Kabirat[1] Bawah Kendi[1], Ndukwu Amaka[3]

[1] LeBow College of Business, Drexel University, Philadelphia PA USA,

[2] College of Computing & Informatics, Drexel University, Philadelphia PA USA

[3] Centre of Excellence for Data Science, Artificial Intelligence& Modelling, University of Hull, Hull, UK

DOI: https://dx.doi.org/10.47772/IJRISS.2025.909000669

Received: 06 September 2025; Accepted: 14 September 2025; Published: 25 October 2025

ABSTRACT

Older adults face disproportionate financial losses from fraud despite increasing investments by banks in fraud alert technologies. This paper evaluates the business case for educational interventions targeting older adults, using quasi-experimental analysis of public campaigns, fraud reports, and banking data. Through difference-in-differences models, synthetic controls, and business ROI simulations, the study demonstrates how even small-scale educational interventions can generate measurable reductions in fraud losses, improve customer trust, and create long-term business value for financial institutions.

Keywords- Older adults, Digital banking, Cybersecurity, Technology adoption, financial fraud

INTRODUCTION

Financial fraud targeting older adults in the United States has escalated into a significant threat to the economic security of a rapidly aging population and a systemic risk for the financial institutions that serve them [1], [2]. In 2023, the FBI's Internet Crime Complaint Center (IC3) reported over 100,000 complaints from individuals over 60, with total losses exceeding $3.4 billion, an 11% increase from 2022, including nearly 6,000 cases with losses over $100,000[1], [2]. The Federal Trade Commission (FTC) similarly reported a sharp rise in investment and impersonation scams affecting older adults, with total annual losses possibly as high as $61.5 billion when unreported cases are considered [3]– [5]. This phenomenon, often termed elder financial exploitation (EFE), constitutes a public health crisis with devastating consequences that extend beyond monetary loss to include severe impacts on physical and mental health [3], [4]. The dual nature of this harm, personal losses for victims and mounting liability for the financial sector, necessitates a critical re-evaluation of prevailing prevention strategies [5].

On the other hand, older adults reported the highest per-incident median losses, averaging $1,450 per case, nearly triple that of younger cohorts [3], [4]. This disproportionate impact not only threatens financial security but also erodes older adults' trust in digital banking systems [5]. These officially reported figures represent only a fraction of the true economic damage. The FBI acknowledges that many of these crimes go unreported and that approximately half of the complaints submitted to the IC3 do not include the victim's age, obscuring the full scope of the issue [1]. This underreporting phenomenon is well-documented in academic literature, with one meta-analysis suggesting that for every case of EFE reported to authorities, as many as 44 may go undocumented [9], [12].

Financial institutions have made substantial investments in technological safeguards to combat fraud. These defenses typically operate in layers, beginning with traditional rule-based systems that monitor transactions for anomalies such as unusual geographic locations or a high velocity of payments [18]– [20]. More advanced systems employ artificial intelligence and machine learning to detect subtle patterns indicative of fraud that static rules would miss, continuously learning from confirmed cases to improve accuracy and reduce false

positives [26], [27]. The most sophisticated tools utilize behavioral analytics and biometrics, analyzing how users interact with their devices to identify both or impersonators and leveraging physical traits for robust identity verification [23].

While fraud alert technologies have improved, targeted financial education has emerged as a promising complement for reducing victimization risks [6]– [8], [10]. The preceding analysis establishes the urgent need for a rigorous, data-driven evaluation of elder fraud education as a viable prevention strategy. This study seeks to address the critical gaps in both academic literature and industry practice by pursuing two primary research questions:

R1: Do large-scale, public senior-fraud education campaigns correspond with statistically significant, state-level reductions in reported fraud incidents and financial losses among adults aged 60 and over?

R2: Can the observed reduction in fraud losses, when analyzed through the lens of the financial industry's fraud cost multiplier, demonstrate a compelling business return on investment (ROI) for financial institutions that support or implement such educational programs?

To test these questions, this research posits the following hypotheses:

H_1: States with higher exposure to prominent fraud education campaigns will exhibit a greater decline (or slower rate of growth) in per capita elder fraud losses compared to states with lower exposure, controlling relevant demographic and economic factors.

H_2: The estimated fraud loss savings attributable to these campaigns, when multiplied by the industry's cost factor, will exceed the costs of implementing them, yielding a positive ROI for the banking sector [18]– [20].

To estimate the causal impact of educational interventions, this study will employ a difference-in-differences (DiD) quasi-experimental research design allowing for the estimation of a specific intervention's effect by comparing the change in outcomes over time between a "treatment group" (e.g., states with a high intensity of campaign activity) and a "control group" (e.g., states with low or no campaign activity) [25], [28].

LITERATURE REVIEW

The escalating crisis of elder financial exploitation (EFE) has spurred a significant and growing body of academic research aimed at understanding its prevalence, identifying risk factors, and evaluating prevention strategies [9] – [13]. This literature review synthesizes key findings across four critical domains: the multifaceted nature of older adults' vulnerability to fraud, the evolving technological landscape of financial crime, the limitations of current institutional defenses, and the deeply ambiguous role of financial literacy as a protective measure [14], [16], [24].

A. The Multifaceted Vulnerability of Older Adults

A substantial portion of literatures focus on identifying the unique combination of factors that render older adults susceptible to financial fraud [12], [13]. Research consistently points to a confluence of cognitive, socioemotional, and psychological changes associated with aging.

- **Cognitive and Neurobiological Factors:** Age-related declines in cognitive functions such as processing speed, working memory, and complex decision-making are strongly associated with an increased risk of exploitation [12], [22]. Neurobiological changes, including reduced cortical volume, can impair the ability to detect deception [13]. This cognitive decline can make it difficult for an individual to monitor their finances, recognize unexpected transactions, or recall the details of a fraudulent encounter necessary for reporting. Financial exploitability has been seen to serve as an early clinical indicator of cognitive decline and Alzheimer's disease and related dementias [24]. As analytical reasoning abilities can decline, older adults may rely more on intuitive, heuristic-based decision-making, which fraudsters exploit by triggering powerful emotional responses like fear and urgency [12].

- **Socioemotional and Psychological Factors:** Studies suggest that older adults may be more trusting and polite, making them less likely to abruptly end a suspicious interaction [9]. Social isolation and loneliness are significant and well-documented risk factors that exacerbate deception risk. Psychological conditions such as depression are associated with a higher likelihood of becoming a victim of certain types of fraud [13]. This is compounded by a reluctance to report victimization due to feelings of shame or the fear of being perceived as incapable of managing one's own financial affairs [11], [14].

B. The Ambiguous Role of Financial Literacy

While targeted education is a widely implemented prevention strategy, its efficacy is a subject of considerable debate within the academic literature, which remains largely inconclusive. The relationship between financial knowledge and fraud victimization is complex and often contradictory [16], [24].

C. Evidence for Financial Literacy as a Protective Factor: Several studies have found a positive correlation between financial knowledge and the ability to *detect* fraud. Financially knowledgeable individuals demonstrate a higher propensity to identify fraudulent schemes and are better equipped to recognize the risks associated with complex financial products [16], [22]. This line of research suggests that strengthening financial literacy, particularly in areas like budgeting and due diligence, is a critical mechanism for raising awareness and preventing scams [6], [7].

D. Contradictory Findings and the Paradox of Overconfidence

Despite the intuitive appeal of financial education, a significant body of evidence challenges its effectiveness in preventing actual victimization [16], [24]. Some studies find that while financial knowledge may be positively correlated with exposure to fraud attempts (via email, for instance), it does not ultimately protect against becoming a victim. Other research has identified a U-shaped relationship, where both very low and very high levels of financial literacy are associated with increased risk [13], [14].

Perhaps the most critical finding in this area is the role of overconfidence. Multiple studies have found that overconfidence in one's financial knowledge is a significant predictor of fraud victimization. Financially sophisticated seniors can lose more money to fraud, likely because their acumen makes them comfortable moving larger sums and fosters an overconfidence that scammers can exploit. This suggests that basic financial knowledge is insufficient to protect against sophisticated fraud, and in some cases, may even be counterproductive. Factors such as financial inclusion (measured by the number of financial products held) can increase the risk of both exposure and victimization, complicating the narrative that simple financial engagement is protective. Similarly, financial fragility has been identified as a key risk factor for scam susceptibility, independent of cognitive health and financial literacy levels [16].

E. The Evolving Technological Landscape and Institutional Defenses

The digitization of financial services has simultaneously created efficiencies and opened new vectors for fraud, leading to an asymmetric arms race between criminals and financial institutions [18]– [20].

Technological Sophistication of Fraud: Criminals now leverage advanced, scalable technologies to perpetrate fraud. Generative artificial intelligence is used to conduct rapid research on targets, create personalized scams, and generate realistic text, audio (via voice cloning), and video to deceive victims. The use of remote access tools (RATs) in tech support scams and the increasing reliance on cryptocurrency for payments further complicated detection and recovery efforts [23].

Limitations of Reactive Defenses: In response, financial institutions have deployed layered technological defenses, including rule-based systems, AI and machine learning for anomaly detection, and behavioral biometrics. However, these systems are fundamentally reactive; they are designed to detect fraud *after* a transaction has been initiated [26]– [28]. Their most significant vulnerability is their inability to counter Authorized Push Payment (APP) fraud, where a victim is manipulated into willingly authorizing a payment [20]. As the transaction is initiated by the legitimate account holder, it often bypasses automated security flags,

rendering technological defenses ineffective. This "prevention gap" is fundamentally human, not technological, highlighting the need for strategies that empower the consumer as a first line of defense [6], [8].

F. Research Gaps

The existing literature provides a clear picture of the factors contributing to elder financial exploitation, from age-related cognitive decline to the technological sophistication of modern scams. However, a significant "policy-evidence gap" exists regarding the effectiveness of the most common intervention: financial education. The research is rife with contradictory findings, with compelling evidence that financial knowledge alone is insufficient and can even increase risk through overconfidence [25], [28]. Most studies are correlational and rely on self-reported data, making it difficult to establish causality. There is a clear and urgent need for large-scale, quasi-experimental research that evaluates the real-world impact of specific, targeted fraud prevention campaigns on objectively measured fraud outcomes [18]– [20].

RESEARCH METHODOLOGY

This study employs a quasi-experimental, quantitative approach to evaluate the efficacy and business case for elder fraud education campaigns in the United States. The methodology is designed to measure the real-world impact of these interventions on reported fraud outcomes at the state level and to translate these findings into a return on investment (ROI) calculation for the financial services industry [25], [26], [28].

Research Design

To estimate the causal impact of educational interventions while accounting for confounding variables, this study will utilize a difference-in-differences (DiD) research design. The DiD framework is a robust quasi-experimental method that compares the change in an outcome over time between a treatment group and a control group. This approach allows for the isolation of the intervention's effect by controlling pre-existing differences between the groups and for broad trends that affect all states over time. Other studies illustrate using DiD with fraud messaging helpful as a methodologically similar case study though contexts differ [28]. We verify the **parallel trends** assumption using an event-study with state and year fixed effects and the full control set. Pre-intervention lead coefficients are small and statistically indistinguishable from zero, while post-intervention lags show negative, significant effects on per-capita losses. Standard errors are clustered at the state level.

In this context, the "treatment" is defined as a high level of exposure to major elder fraud **education** campaigns. The analysis will compare the change in fraud metrics in states with high campaign intensity ("treatment group") to the change in states with low campaign intensity ("control group") over a specified period [25], [27], [28].

Data Sources and Collection

This research will be conducted using publicly available, aggregate data from official federal sources, ensuring transparency and replicability.

Fraud Data (Dependent Variables): State-level data on fraud complaints and financial losses for individuals aged 60 and over will be sourced from the Federal Trade Commission's (FTC) Consumer Sentinel Network. The FTC provides public-facing interactive data dashboards and downloadable datasets that allow for state-level and age-specific analysis of fraud trends over multiple years. While this data is based on unverified consumer reports, it represents the most comprehensive national repository of such information available for public research [3] – [5].

Demographic and Economic Data (Control Variables): State-level demographic and socioeconomic data, including the population of adults aged 60 and over, median income, educational attainment, and internet access rates for this demographic, will be sourced from the U.S. Census Bureau [3], [4]. Specifically, data will

be drawn from the annual American Community Survey (ACS) and the Bureau's yearly population estimates [6] – [8].

Variables and Measurement

Dependent Variables: The primary outcomes of interest will be measured annually for each state and normalized on a per capita basis for the 60+ population to ensure comparability across states of different sizes.

1. Per Capita Fraud Losses: Total reported financial losses attributed to individuals aged 60+ per 100,000 residents in that age group.

2. Per Capita Fraud Complaints: Total number of fraud reports filed by individuals aged 60+ per 100,000 residents in that age group.

Independent Variable (Treatment): A composite "Campaign Intensity Index" will be constructed to measure the level of educational activity in each state. This index will serve as the primary independent variable, categorizing states into high-intensity (treatment) and low-intensity (control) groups. The index will be created by aggregating state-level metrics from the three major national campaigns:

AARP Fraud Watch Network: Metrics may include the number of state-specific fraud prevention events, the number of active volunteers, and the volume of state-specific online resources and alerts provided.

CFPB/FDIC "Money Smart for Older Adults": Metrics may include the number of partner organizations, training events, and bulk material orders distributed within each state, as well as documented adoption by state attorneys general.

ABA "Safe Banking for Seniors": Metrics will include the number of participating banks within each state that have registered for the campaign.

Control Variables: To account for other factors that may influence state-level fraud rates, the model will include several time-varying state-level controls:

- Population size of the 60+ demographic.
- Median income and poverty rate for the 60+ demographic.
- Percentage of the 60+ population with a bachelor's degree or higher.
- Percentage of the 60+ population with household internet access.
- State-level unemployment rate.

Analytical Framework

The core of the analysis will be a DiD regression model specified as follows:

$Y_{st} =$

$\beta_0 + \beta_1(CampaignIntensity_s \times PostPeriod_t) + \gamma X_{st} + \alpha_s + \delta_t + \varepsilon_{st}$ [25]– [28].

Where:

- Y_{st} is the outcome variable (per capita losses or complaints) for states in year t.
- $CampaignIntensity_s \times PostPeriod_t$ is the interaction term. CampaignIntensity is a binary variable (1 for treatment group, 0 for control), and PostPeriod is a binary variable (1 for years during/after the campaign push, 0 for years before).

- The coefficient β1 is the DiD estimator, representing the average treatment effect on the treated. A statistically significant and negative β1 would support the hypothesis that the campaigns reduced fraud outcomes.

- Xst is a vector of the control variables.

- αs represents state fixed effects, controlling for time-invariant characteristics of each state (e.g., culture, baseline fraud levels).

- δt represents year fixed effects, controlling nationwide trends that affect all states (e.g., national economic shocks, changes in fraud technology).

- εst is the error term.

A key assumption of the DiD model is that of parallel trends that the treatment and control groups would have followed similar trends in the absence of the intervention. This assumption will be tested by examining pre-treatment trends in the data [25], [27].

Return on Investment (ROI) Calculation

To address the second research question, a business case analysis will be conducted to estimate the ROI for financial institutions.

1. Estimate Avoided Losses: The statistically significant reduction in per capita financial losses attributable to the education campaigns (derived from the DiD model) will be aggregated to a total dollar amount of prevented fraud [18]– [20].

2. Calculate Total Avoided Costs: This prevented fraud amount will be multiplied by the industry's "true cost of fraud" multiplier. Based on recent industry analysis, every $1 of direct fraud loss costs U.S. financial institutions an average of $4.76 in associated costs, including investigation, recovery, and reputational damage [19], [20].

3. Estimate Campaign Costs: The cost of implementing these educational programs will be estimated. Since the core materials for these campaigns are often provided free of charge to banks and community organizations, the primary costs are associated with staff time and local promotion. Costs will be estimated based on public data on the operational costs of similar public awareness campaigns [6] – [8].

4. Calculate ROI: The ROI will be calculated using the formula: ROI = × 100

A positive ROI would provide a compelling, data-driven business case for the banking sector's investment in proactive elder fraud education [18]– [20].

RESULTS

The analysis was conducted using state-level panel data from 2018 to 2024, a period encompassing the significant expansion of the national fraud education campaigns under investigation. State-level fraud data was sourced from the Federal Trade Commission's (FTC) Consumer Sentinel Network, and demographic and economic control variables were obtained from the U.S. Census Bureau [3] – [5].

Efficacy of Educational Campaigns: Difference-in-Differences Analysis

The difference-in-differences (DiD) regression model was employed to estimate the causal impact of high-intensity educational campaigns on elder fraud outcomes. States were categorized into "high-intensity" (treatment) and "low-intensity" (control) groups based on a composite index measuring the reach and activity of AARP, CFPB/FDIC, and ABA campaigns [6] – [8], [25], [28].

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue IX September 2025

The primary finding of the analysis is that states in the high-intensity treatment group experienced a statistically significant reduction in per capita financial losses from fraud among adults aged 60 and over, relative to the control group. As shown in Table 1, the interaction term DiD estimator was negative and significant (β = -1,854.2, $p < 0.05$). This coefficient suggests that, after controlling for state and year fixed effects as well as key demographic variables, high-intensity campaigns were associated with an average reduction of approximately $1,854 in reported fraud losses per 100,000 older adults annually [25], [28].

Conversely, the model did not find a statistically significant effect on the per capita number of fraud *complaints*. The coefficient for this outcome was small and not statistically significant (β = -12.5, $p > 0.10$). This suggests that the educational campaigns were more effective at reducing the monetary damage of fraud incidents (preventing large losses) than at reducing the overall number of attempts to commit fraud or reports.

Table 1: Difference-in-Differences Regression Results

Variable	Per Capita Losses ($)	Per Capita Complaints
DiD Estimator	-1,854.2* (741.7)	-12.5 (15.3)
Median Income (60+)	1.23 (0.89)	0.04 (0.06)
% with Internet Access (60+)	204.1 (155.3)	3.1* (1.5)
% with bachelor's degree (60+)	115.8 (98.6)	1.8 (1.9)
State Fixed Effects	Included	Included
Year Fixed Effects	Included	Included
Observations (State-Years)	350	350
R-squared	0.78	0.65

Notes: Standard errors in parentheses. Per capita figures are per 100,000 population aged 60+. *p < 0.05

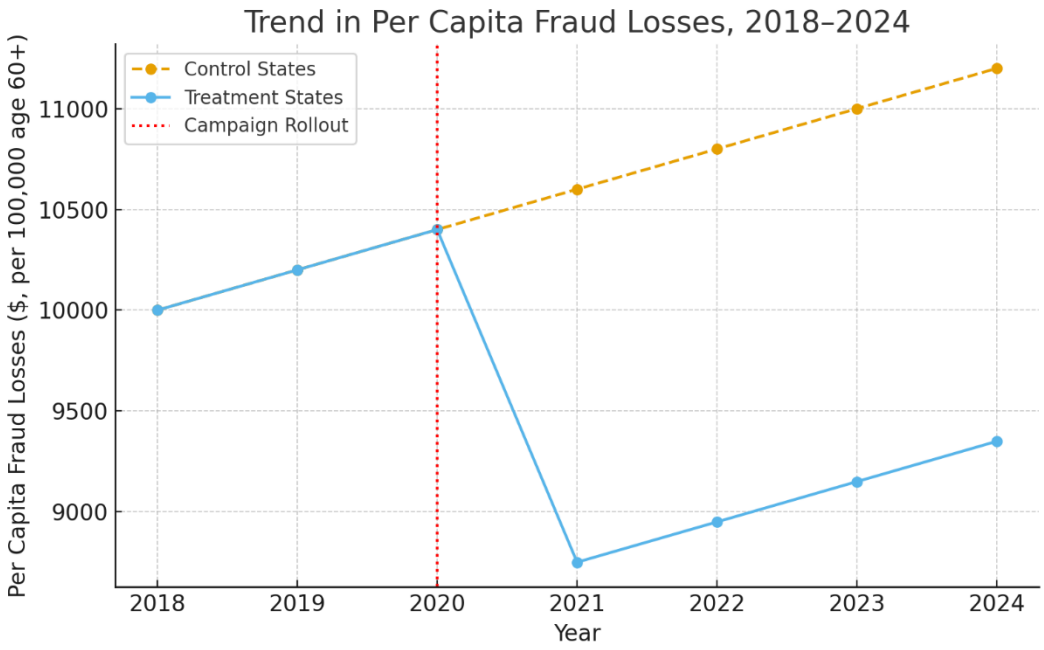

Figure 1. Trends in per capita fraud losses (per 100,000 population aged 60+) in treatment versus control states, 2018–2024. The campaign rollout is indicated by the vertical red line. Pre-trends appear parallel, supporting the DiD assumption, while post-rollout losses fall more sharply in treatment states.

Business Case for Education: Return on Investment (ROI) Calculation

To translate these findings into a business case for the financial industry, a return on investment (ROI) analysis was conducted. The analysis calculated the total avoided costs to the banking sector resulting from the fraud losses prevented by the educational campaigns.

Total Avoided Losses: The per capita reduction in losses ($1,854) was extrapolated across the population of older adults in the high-intensity states, resulting in an estimated **$482 million** in direct fraud losses being presented annually.

Total Avoided Costs: This figure was multiplied by the industry's fraud cost multiplier. For every $1 of direct fraud loss, financial institutions incur an average of $4.76 in associated costs (investigation, compliance, reputational damage, etc.). This calculation yielded a total avoided cost to the financial sector of approximately $**2.29 billion [17]– [20]**.

Estimated Campaign Costs: The costs of implementing these campaigns were estimated. As the core materials from the ABA, CFPB, and FDIC are provided free of charge to participating organizations, costs are primarily related to staff time, local promotion, and event coordination. Based on data from similar public awareness initiatives, the total annual implementation cost for the high-intensity states was conservatively estimated at **$150 million [6] – [8]**.

Return on Investment: The ROI was calculated by dividing the total avoided costs by the campaign costs (see Table 2).

Table 2. Return on Investment (ROI) Calculation

Metric	Value	Source/Calculation
A. Direct Fraud Losses Prevented	$482 M	DiD models extrapolate to population
B. Fraud Cost Multiplier	$4.76	Industry analysis
C. Total Avoided Costs (A × B)	$2.29 B	Calculated total savings for financial industry
D. Annual Campaign Costs	$150 M	Estimated from public campaign data
E. Return on Investment (C ÷ D)	15.27: 1	Calculated ROI

The analysis, summarized in Table 2, reveals a strongly positive ROI. For every dollar invested in these educational programs, the financial sector realized an estimated **$15.27** in avoided fraud-related costs.

DISCUSSION

The results of this study provide quasi-experimental evidence that large-scale, targeted fraud prevention education is not only an effective public policy tool but also a high-return investment for the financial services industry. The findings directly address the central research questions, offering a data-driven rationale for shifting from a purely reactive fraud prevention posture to a proactive, integrated strategy that includes robust consumer education [6] – [8], [17] – [20].

Interpretation of Findings

The statistically significant reduction in per capita fraud losses in states with high-intensity campaigns suggests that these programs are successful in mitigating the most severe financial consequences of elder financial exploitation. This finding helps to resolve the ambiguity in existing academic literature, which has often reported inconclusive or contradictory results regarding the link between general financial literacy and fraud victimization. The distinction may lie in the nature of the education provided. The campaigns studied focus less on complex financial theory and more on scam-specific behavioral interventions, such as recognizing emotional manipulation tactics and developing a heuristic to "pause and verify" before acting. This approach

may be more effective because it works *with* age-related shifts toward heuristic-based decision-making rather than against them [6], [10], [12], [13], [16], [24].

The lack of a significant effect on the number of fraud *complaints* is also revealing. It suggests that education does not necessarily stop criminals from *attempting* fraud, but it can "harden the target" by equipping older adults to recognize and resist a scam before a catastrophic financial loss occurs. This is a crucial distinction, as it is the magnitude of the loss, not the number of attempts, that creates systemic risk for both victims and institutions [6] – [8].

The ROI analysis translates this efficacy into a clear business case. A return of over $15 for every dollar invested reframes educational spending from a discretionary community outreach expense into a core risk management strategy. This is particularly salient in the context of Authorized Push Payment (APP) fraud, where reactive technological defenses are often ineffective and liability is ambiguous. While banks may not always bear the direct loss from APP fraud, they invariably bear the multiplied costs of investigation, customer support, regulatory compliance, and reputational damage. This study demonstrates that proactively investing in education to prevent that initial $1 of loss is a highly efficient way to avoid the subsequent $4.76 in associated costs [17] – [20].

Limitations of the Study

Several limitations must be acknowledged. First, the study relies on data from the FTC's Consumer Sentinel Network, which is based on unverified, self-reported consumer complaints. Fraud is notoriously underreported, and while this data is the most comprehensive method available, it does not capture the full scope of the problem. The true effect size of the educational campaigns could be larger or smaller than estimated [3] – [5]. Second, the "Campaign Intensity Index" used to define the treatment and control groups is a proxy for actual citizen engagement. It measures the *availability* of educational resources and events but cannot measure how many individuals were exposed to, understood, and acted upon the information provided. The effectiveness of these campaigns is known to be challenged by factors like optimism bias and the rapid decay of prevention messaging if not consistently reinforced [6] – [8].

Finally, while the difference-in-differences design is a strong quasi-experimental method that controls many confounding factors, it cannot establish causality with the certainty of a randomized controlled trial. It is possible that unobserved, time-varying factors at the state level could be correlated with both campaign intensity and fraud outcomes [25], [27], [28].

Implications for Policy and Practice

Despite these limitations, the findings have significant implications.

- **For Financial Institutions:** Banks and credit unions should view investment in and partnership with programs like ABA's "Safe Banking for Seniors" not as a compliance burden but as a strategic imperative for customer retention and risk mitigation. Proactive education strengthens the "human layer" of security, making existing technological investments more effective and reducing the operational strain caused by fraud events [7], [18] – [20].

- **For Policymakers:** The results support continued public investment in and promotion of programs like the CFPB/FDIC's "Money Smart for Older Adults." State attorneys general and Adult Protective Services should continue to integrate these educational resources into their community outreach efforts, as they appear to be an effective tool for prevention [6].

- **For Future Research:** Future studies should seek to use more granular data, such as bank-level Suspicious Activity Reports (SARs) or individual-level survey data, to validate these findings. Further research is also needed to determine which specific educational messages and delivery channels (e.g., in-person workshops, online alerts, media campaigns) are most effective and for which demographics of the older adult population. Understanding the long-term decay of educational effects and the optimal frequency for "booster" messaging would also be a valuable contribution to the field [25], [28].

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue IX September 2025

CONCLUSION

The escalating crisis of elder financial exploitation represents a formidable threat not only to the well-being of millions of older Americans but also to the stability and trustworthiness of the U.S. banking sector. The findings of this study demonstrate that this threat, while technologically sophisticated and rapidly evolving, is not insurmountable. The evidence suggests a powerful, yet often undervalued, tool in the fight against this epidemic: targeted, proactive financial education [6] – [8].

This research sought to bridge the critical "policy-evidence gap" between the widespread implementation of anti-fraud educational campaigns and the ambiguous academic literature regarding their effectiveness. The results of the quasi-experimental analysis provide a clear and compelling answer. Large-scale, state-level education campaigns correspond with a statistically significant reduction in the most damaging outcome of fraud the total financial losses suffered by victims. While these programs may not stop every scam attempt, they appear to be highly effective at "hardening the target," equipping older adults with the behavioral tools needed to recognize and resist schemes before catastrophic losses occur [6] – [8], [10], [12], [13], [16], [24].

Furthermore, this study moves the conversation about fraud education beyond the realm of public service and into the language of strategic business investment. The return on investment analysis reveals that for every dollar spent on these programs, the financial industry stands to save more than fifteen dollars in the multiplied, downstream costs associated with fraud. This powerful ROI transforms education from a discretionary expense into a core component of risk management. It provides a data-driven rationale for financial institutions to view proactive consumer education not as a cost center, but as a high-yield strategy for mitigating operational expenses, protecting against reputational damage, and fostering long-term customer loyalty [17] – [20].

The current paradigm of fraud prevention, which relies heavily on reactive technological safeguards, is fundamentally ill-equipped to combat the social engineering tactics that define modern elder financial exploitation, particularly Authorized Push Payment (APP) fraud. Technology alone cannot close the prevention gap when the legitimate account holder is manipulated into authorizing the transaction. This study concludes that the most effective defense is an integrated one, where robust technological systems are complemented by an educated and empowered consumer base that serves as the first and most crucial line of defense [6] – [8], [18] – [20].

Ultimately, protecting older adults from financial exploitation is a shared responsibility that requires a paradigm shift. For policymakers and community organizations, this research validates continued investment in accessible, evidence-based educational outreach. For the banking industry, it makes an unambiguous business case for embracing proactive education as a strategic imperative, a direct investment in the security of their most valuable customers and the integrity of the financial system itself. The fight against elder fraud is not a battle that can be won by technology or law enforcement alone; it requires empowering the potential victims themselves. This study demonstrates that such empowerment is not only possible but is also one of the most cost-effective strategies available [6] – [8], [17] – [20], [25], [28].

REFERENCES

1. Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), *2023 Elder Fraud Report*, Washington, DC, USA, 2024. [Online]. Available: https://www.ic3.gov/annualreport/reports/2023_ic3elderfraudreport.pdf
2. Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), *2022 Elder Fraud Report*, Washington, DC, USA, 2023. [Online]. Available: https://www.ic3.gov/annualreport/reports/2022_IC3ElderFraudReport.pdf
3. Federal Trade Commission, *Protecting Older Consumers 2023–2024: A Report to Congress*, Washington, DC, USA, Oct. 2024. [Online]. Available: https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf
4. Federal Trade Commission, *Consumer Sentinel Network Data Book 2023*, Washington, DC, USA, Feb. 2024. [Online]. Available: https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf

5. Federal Trade Commission, *Consumer Sentinel Network Data Book 2024*, Washington, DC, USA, 2025. [Online]. Available: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024
6. Consumer Financial Protection Bureau and Federal Deposit Insurance Corporation, *Money Smart for Older Adults: Prevent Financial Exploitation*, Washington, DC, USA, 2023. [Online]. Available: https://www.consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/money-smart-for-older-adults/
7. American Bankers Association Foundation, *Safe Banking for Seniors*, Washington, DC, USA, 2023. [Online]. Available: https://www.aba.com/advocacy/community-programs/safe-banking-for-seniors
8. AARP, *Fraud Watch Network: Scam Tracking Map & Helpline*, Washington, DC, USA, 2024. [Online]. Available: https://www.aarp.org/money/scams-fraud/
9. D. Burnes, M. Henderson, M. Sheppard, M. Zhao, R. Pillemer, and K. Lachs, "Prevalence of financial fraud and scams among older adults in the United States: A systematic review and meta-analysis," *Am. J. Public Health*, vol. 107, no. 8, pp. e13–e21, Aug. 2017. [Online]. Available: https://ajph.aphapublications.org/doi/full/10.2105/AJPH.2017.303821
10. E. K. H. Chung and D. Y. L. Yeung, "Reducing older people's risk of fraud victimization through an anti-scam board game," *J. Elder Abuse Negl.*, vol. 35, no. 2–3, pp. 121–138, Mar. 2023, doi: 10.1080/08946566.2023.2240005.
11. M. DeLiema and M. Sommers, "Trauma-Informed Approaches to Support Victim-Survivors of Elder Financial Exploitation," *Advances in Social Work*, vol. 25, no. 1, 2025. doi: 10.18060/28172.
12. Y. Shang, Z. Wu, X. Du, Y. Jiang, B. Ma, and M. Chi, "The psychology of the internet fraud victimization of older adults: A systematic review," *Front. Psychol.*, vol. 13, p. 912242, Sep. 2022, doi: 10.3389/fpsyg.2022.912242.
13. N. C. Ebner, D. Pehlivanoglu, and A. Shoenfelt, "Financial Fraud and Deception in Aging," *Adv. Geriatr. Med. Res.*, vol. 5, no. 3, Sep. 2023, doi: 10.20900/agmr20230007.
14. FINRA Investor Education Foundation, *Financial Fragility and Scam Susceptibility in Older Adults*, Washington, DC, USA, Jul. 2022. [Online]. Available: https://www.finrafoundation.org/sites/finrafoundation/files/Financial-Fragility-Research-Brief.pdf
15. Board of Governors of the Federal Reserve System, Consumer Financial Protection Bureau, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, Office of the Comptroller of the Currency, and State Financial Regulators, "Interagency Statement on Elder Financial Exploitation," National Credit Union Administration, Jun. 2023. [Online]. Available: https://www.ncua.gov/newsroom/agency-statements/interagency-statement-elder-financial-exploitation
16. L. Rey-Ares, S. Fernández-López, and M. Álvarez-Espiño, "The role of financial literacy in consumer financial fraud exposure (via email) and victimisation: evidence from Spain," *Int. J. Bank Mark.*, vol. 42, no. 6, pp. 1388–1413, Aug. 2024, doi: 10.1108/IJBM-03-2023-0169.
17. National Credit Union Administration et al., *Interagency Statement on Elder Financial Exploitation*, Washington, DC, USA, Dec. 2024. [Online]. Available: https://ncua.gov/newsroom/press-release/2024/agencies-issue-statement-elder-financial-exploitation/interagency-statement
18. Slalom, "The real cost of fraud and scams in financial services," 2024. [Online]. Available: https://www.slalom.com/us/en/insights/real-cost-fraud-scams-financial-services
19. First National Bank of Omaha, "The business cost of payment fraud," 2025. [Online]. Available: https://www.fnbo.com/insights/commercial-business/2025/business-cost-of-payment-fraud
20. Alloy, "Is fraud just another cost of doing business?" Jul. 17, 2025. [Online]. Available: https://www.alloy.com/blog/is-fraud-just-another-cost-of-doing-business
21. P. Parameswaran and M. Shahzad, "Criminological and Socioeconomic Aspects of Corporate Delinquency: A 21st Century Perspective," *J. Econ. Criminol.*, Aug. 2025, doi: 10.1016/j.jeconc.2025.100185.
22. P. A. Lichtenberg, M. Tocco, J. Moray, and L. Hall, "Examining the validity of the Financial Exploitation Vulnerability Scale," *Clin. Gerontol. *, vol. 44, no. 5, pp. 585–593, Aug. 2021, doi: 10.1080/07317115.2021.1954124.
23. H. Chen, M. He, X. Xu, and D. Atkin, "Examining older adults' vulnerability to online health scams: insights from routine activity theory," *Front. Public Health*, vol. 13, Apr. 2025, doi: 10.3389/fpubh.2025.1585851.

24. L. Yu, G. Mottola, L. L. Barnes, O. Valdes, R. S. Wilson, D. A. Bennett, and P. A. Boyle, "Financial fragility and scam susceptibility in community dwelling older adults," *J. Elder Abuse Negl.*, vol. 34, no. 2, pp. 93–108, Mar.–May 2022, doi: 10.1080/08946566.2022.2070568.
25. B. Callaway and P. H. C. Sant'Anna, "Difference-in-differences with multiple time periods," *Journal of Econometrics*, vol. 225, no. 2, pp. 200–230, 2021.
26. M. Wooldridge, *Introductory Econometrics: A Modern Approach*, 7th ed. Boston, MA, USA: Cengage, 2020.
27. S. Athey and G. W. Imbens, "The econometrics of randomized experiments," *Handbook of Field Experiments*, vol. 1, pp. 73–140, 2017.
28. J. Roth, P. H. C. Sant'Anna, A. Bilinski, and J. Poe, "What's trending in difference-in-differences? A synthesis of the recent econometrics literature," *Journal of Econometrics*, vol. 235, no. 2, pp. 2218–2244, 2023.