Volume 2 Issue 2

# International Journal of Social Work and Development Studies (IJSDS)

DEPARTMENT OF SOCIAL WORK
FACULTY OF SOCIAL SCIENCES
RIVERS STATE UNIVERSITY
EMOHUA CAMPUS, P.M.B 5080, PORT HARCOURT
RIVERS STATE NIGERIA

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

# International Journal of Social Work and Development Studies (IJSDS)

Vol 2 Issue 2

editor@ijsds.org
www.ijsds.org
editor.ijsds@gmail.com
+234 808 022 4405

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

# PROTECTING VULNERABLE POPULATIONS FROM CYBER FRAUD: AN EMERGING ROLE FOR SOCIAL WORKERS

**Femi Folorunsho**
Ball State University,
Media Department
Muncie, IN, USA
(orcid: 0009-0005-0883-0062)

**Innocent C. Ugochukwu**
Ball State University,
Educational Studies
Muncie, IN, USA

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

## ABSTRACT

Cyber fraud against older adults is often framed as a problem of awareness, yet the evidence used to guide prevention is dominated by administrative counts of complaints and financial loss. This study compares two separately administered national reporting systems: the Federal Bureau of Investigation Internet Crime Complaint Center (IC3) 2023 Elder Fraud Report and the Federal Trade Commission (FTC) Consumer Sentinel Network Data Book 2023. The IC3 source covers 101,068 complaints by adults over 60 and $3.428 billion in reported losses; the FTC source covers 2,566,261 fraud reports and more than $10 billion in reported losses. Descriptive decomposition, derived severity ratios, three-year trend analysis, and cross-source pattern triangulation were used. In IC3 data, mean loss rose monotonically across age bands, and adults over 60 accounted for 24.1% of age-identified complaints but 41.9% of associated losses. In FTC data, the share of fraud reports indicating monetary loss fell from 44% among adults aged 20 to 29 to 22% among adults aged 80 and older, while median loss rose from $480 to $1,450. These results support vulnerability of consequence rather than generalised susceptibility. Both systems identified investment fraud as the highest-severity major category: IC3 investment fraud represented 6.4% of over-60 complaints but 36.3% of losses, and FTC investment-related fraud had the highest median loss among the ten largest fraud categories ($7,768). Within 626 IC3 Recovery Asset Team incidents, 55.1% of the reported dollar value was frozen; frozen funds equalled 0.94% of all reported over-60 losses, and freezing is not the same as return of funds. Neither published report tabulates psychological, relational, housing, health, or service-referral outcomes. A severity-informed social work response is proposed, centred on relational guardianship, shame-sensitive disclosure, crisis assessment, recovery navigation, and digital reintegration.

**Keywords:** elder fraud, cyber fraud, social work, financial exploitation, administrative data, digital inequality, victimisation

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

## 1.0 INTRODUCTION

Digital participation is now embedded in banking, healthcare, benefit administration, employment, and social connection. This expansion creates access and convenience while also placing people within reach of offenders who manipulate trust at scale. Cyber fraud is therefore not simply a technical security problem. It is a form of social victimisation that can convert isolation, bereavement, financial insecurity, cognitive change, and trust in institutions into mechanisms of exploitation.

Older adults occupy a distinctive position in this landscape. Popular discussion often assumes that older adults are inherently more likely to be deceived. The empirical record is more complicated. Some studies find that older people are not victimised more frequently than younger people, while administrative reports consistently show substantially greater losses when victimisation succeeds (DeLiema et al., 2018; Ross et al., 2014). The distinction between frequency and consequence matters. A generalised susceptibility narrative risks reproducing ageist assumptions and encouraging paternalistic restrictions on autonomy. A consequence-based account instead focuses attention on accumulated assets, retirement insecurity, reduced opportunity to rebuild savings, and the social conditions that increase the impact of loss.

The public systems used to monitor fraud were designed primarily for law enforcement, consumer protection, trend detection, and financial interdiction. They measure complaint counts, monetary loss, crime category, payment mechanism, and jurisdiction. These measures are indispensable, but they provide only a partial account of harm. Research with victims documents anxiety, depression, sleep disruption, self-blame, family conflict, social withdrawal, and prolonged grief, particularly after relationship-based fraud (Button et al., 2012; Golladay & Holtfreter, 2016; Whitty & Buchanan, 2015). These consequences are not peripheral. They shape reporting, recovery, repeat victimisation, and continued participation in digital life.

Measurement choices influence which problems become visible to policy and which professions are mobilised to respond. Classification systems are institutional artefacts built to support particular decisions (Bowker & Star, 1999; Kitchin, 2014). When fraud is counted principally as money lost, the response architecture privileges police, regulators, banks, and platforms. When grief, shame, housing instability, family conflict, and social withdrawal remain unmeasured, professions equipped to address those outcomes are not incorporated into routine response.

This study addresses that problem through comparative secondary analysis of two national administrative systems. The primary source is the IC3 2023 Elder Fraud Report, which provides detailed data about adults over 60. The second source is the FTC 2023 Consumer Sentinel Network Data Book, which provides age-specific proportions reporting loss and age-specific median losses. The two systems differ in scope, contributors, classifications, and loss measures. Those differences provide an opportunity for triangulation. If the same age-severity pattern and the same high-severity fraud category appear in two separately administered systems using different statistics, the inference is more robust than a conclusion based on a single agency report. Here, "separately administered" refers only to institutional independence: because some reports may be shared between the systems, the two sources are not statistically independent samples.

The study asks:

**RQ1.** How are complaint volume and financial loss distributed across age groups?

**RQ2.** How do reported prevalence (a category's share of over-60 IC3 complaints) and financial severity (its share of reported loss and its mean loss per complaint)

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

diverge across fraud categories affecting adults over 60?

**RQ3.** What changes in complaint volume and severity occurred between 2021 and 2023?

**RQ4.** What proportion of reported over-60 losses is frozen through the IC3 Recovery Asset Team's Financial Fraud Kill Chain?

**RQ5.** Does FTC Sentinel data reproduce the principal IC3 patterns concerning age, severity, and investment fraud?

**RQ6.** What consequential harm dimensions are absent from the published statistics of both administrative systems, and what follows for social work practice?

The article contributes in three ways. Empirically, it distinguishes exposure, loss incidence, and loss severity. Methodologically, it triangulates a mean-based elder-specific system with a median-based general consumer system without treating non-equivalent statistics as interchangeable. Professionally, it identifies a measurable point at which financial response ends and psychosocial need remains.

## 2.0 LITERATURE REVIEW

### 2.1. Fraud as Persuasive and Relational Crime

Fraud scholarship has moved beyond explanations centred on carelessness. Relationship-based fraud develops through staged persuasion, in which identity construction, grooming, incremental requests, and emotional commitment precede extraction (Whitty, 2013). Investment, authority-impersonation, and advance-fee schemes similarly combine urgency, scarcity, reciprocity, and institutional cues (Button & Cross, 2017; Fischer et al., 2013). Banking-fraud research also locates the decisive mechanism in trust management rather than technical intrusion (Jansen & Leukfeldt, 2016).

These schemes frequently suppress consultation. A purported relative asks for secrecy, a romantic contact frames family scepticism as opposition to the relationship, and an impersonator imposes urgency that prevents independent verification. This pattern gives relational guardianship particular importance. A trusted person consulted before a transfer may prevent harm more effectively than technical knowledge alone.

Generative artificial intelligence increases this asymmetry by improving linguistic fluency, producing synthetic profile images that defeat reverse-image checks, and lowering the cost of personalised contact (Cross, 2022; Hazell, 2023). Romance-based deception is also being industrialised through enterprise platforms, scripted workflows, and paid operators who manage intimate conversations at scale (Wang & Topalli, 2024). The implication is not that detection is impossible, but that prevention based on grammar errors or superficial anomalies will become progressively weaker.

### 2.2. Older Adults, Risk, and Consequence

Elder financial exploitation research identifies cognitive impairment, isolation, bereavement, financial strain, and dependency as relevant conditions, but these factors do not justify a categorical assumption of incapacity (Burnes et al., 2017; Lichtenberg, 2016). Decision quality may decline before clinical impairment becomes evident, yet many older adults retain strong judgement and are targeted because they possess assets or because offenders select contexts of acute vulnerability (Boyle et al., 2012; Judges et al., 2017).

A better analytic distinction is between vulnerability to exposure, vulnerability to successful deception, and vulnerability to consequence. Younger adults may encounter or report more attempted fraud, while older adults can sustain more severe losses when fraud succeeds. Consequence is amplified by retirement, fixed income, healthcare expenses, housing dependence,

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

and a shorter time horizon for rebuilding savings.

### 2.3. Psychosocial Harm and Secondary Victimisation

Fraud produces economic, psychological, relational, and civic harm. Victims report anxiety, depression, sleep disturbance, physical health decline, family conflict, and suicidal ideation (Button et al., 2012). Identity theft creates a prolonged administrative burden and persistent hypervigilance (Golladay & Holtfreter, 2016). Romance fraud produces both financial loss and the loss of a subjectively real relationship, creating grief without social recognition (Buchanan & Whitty, 2013; Whitty & Buchanan, 2015).

Blame compounds these harms. Fraud discourse often implies that a vigilant person would have avoided victimisation, locating causal responsibility in the target rather than the offender (Cross, 2015). Anticipated judgement suppresses disclosure and delays reporting, reducing the chance of recovery. Victims may then encounter fragmented institutions with narrow mandates, repeated requests to recount the incident, and little psychosocial support. This has been described as secondary victimisation and can be interpreted as institutional betrayal when systems expected to protect instead intensify harm (Cross, 2018; Cross et al., 2016; Smith & Freyd, 2014).

### 2.4. Why Social Work Matters

The conditions associated with fraud exposure are already central to social work assessment. Social workers evaluate isolation, bereavement, financial stress, housing instability, cognitive change, family conflict, and access to support. The consequences of victimisation are similarly within established competence: crisis intervention, trauma-informed care, grief work, benefits navigation, family mediation, advocacy, and community education.

The profession has nevertheless remained marginal to cyber-fraud response. Fraud is administratively classified as property or consumer crime, digital harm is often perceived as requiring technical expertise, and fraud rarely appears as the presenting problem. Clients may instead present with depression, arrears, family dispute, or unexplained financial depletion. Without a routine assessment prompt, the initiating event remains undisclosed.

### 2.5. Theoretical Framework

Routine activity theory argues that victimisation occurs where a motivated offender, a suitable target, and the absence of capable guardianship converge (Cohen & Felson, 1979). In digital settings, guardianship can be technological, institutional, or relational (Leukfeldt & Yar, 2016; Reyns, 2013; Yar, 2005). For persuasion-based fraud, social guardianship is especially important because offenders deliberately isolate targets from advice.

Ecological systems theory locates individual action within interacting levels of environment (Bronfenbrenner, 1979). Fraud risk therefore cannot be reduced to personal knowledge. Family communication, bank procedures, platform design, service availability, consumer-protection law, and cultural narratives about gullibility all shape outcomes.

Digital inequality scholarship further distinguishes access from skills and outcomes (Hargittai, 2002; Helsper, 2012; Scheerder et al., 2017; van Dijk, 2020). People with equivalent connectivity do not receive equivalent benefit or protection. Cyber fraud is a third-level inequality because the ability to convert digital access into benefit without catastrophic loss depends on social resources, verification support, and institutional protection. Research on security-information seeking among older adults shows that protective knowledge often circulates through informal and uneven channels (Nicholson et al., 2019).

Together, these perspectives predict that individual awareness campaigns will underperform when they are not accompanied by relational guardianship, insti-

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

tutional recovery, and psychosocial support.

## 3.0. METHODOLOGY

### 3.1. Design and Data Sources

The study uses comparative secondary analysis of publicly released aggregate administrative data. The primary dataset is the FBI IC3 *2023 Elder Fraud Report* (Federal Bureau of Investigation, 2024). IC3 received 101,068 complaints from people over 60 in 2023, with $3,427,717,654 in reported loss. The report provides counts and losses by fraud type, age band, state, cryptocurrency descriptor, and three-year trend. The complaint, not the individual, is the unit of analysis. A person may file more than once, and only about half of the more than 880,000 IC3 complaints received in 2023 contained age information.

The comparative source is the FTC *Consumer Sentinel Network Data Book 2023* (Federal Trade Commission, 2024). Sentinel recorded 5,392,028 consumer-protection reports, including 2,566,261 fraud reports and 1,036,903 identity-theft reports. Sentinel combines reports filed directly with the FTC with reports from governmental and nongovernmental contributors. Reports are unverified and are not generated from a probability survey. Dollar-loss calculations include reported losses from $1 to $999,999.

The systems overlap conceptually but cannot be pooled. IC3 emphasises internet-enabled crime and reports an elder-specific over-60 category. FTC Sentinel spans a broader consumer-protection domain and reports narrower age bands. Unknown overlap among contributing reports creates a risk of double counting. The FTC is therefore used as a separately administered directional robustness check, not as an additive dataset or a statistically independent sample.

*Document scope.* The analysis examined the two published reports and the agency web pages that describe them. IC3 and FTC complaint intake forms, data dictionaries, and record-level data were not examined. Statements about absent harm dimensions therefore refer to what the published reports tabulate, not to what the agencies' intake systems may collect, for example in free-text complaint narratives.

### 3.2. Measures and Analysis

For IC3 data, mean loss per complaint was derived by dividing aggregate reported loss by complaint count. Inputs were taken from the published tables listed in Appendix A, which gives source page locators for Tables 1–5, the values entered, each formula, and the result. Derived means were computed from the full-dollar values printed in the source and rounded to the nearest dollar; percentages and percentage changes were rounded to one decimal place, except aggregate freeze coverage, which is reported to two decimal places; aggregate losses in the text are rounded to the nearest $0.1 million or $0.001 billion. Both reports were accessed from the issuing agencies' websites; the values used were last checked on October 22, 2026. Complaint share, loss share, cumulative loss concentration, annual percentage change, and recovery coverage were also calculated. Severity ratios are interpreted as category-level burden indicators, not typical individual losses. In this article, "reported prevalence" means a category's share of over-60 IC3 complaints (category complaints ÷ 101,068). It describes the composition of complaints received, not the population prevalence of victimisation. Two recovery ratios were calculated: the incident-level freeze rate (funds frozen ÷ reported loss in Financial Fraud Kill Chain incidents) and aggregate freeze coverage (funds frozen ÷ all reported over-60 loss).

For FTC data, the analysis used total fraud reports, aggregate reported fraud loss, the percentage of reports indicating monetary loss by selected age group, median loss among reports indicating loss, and the median for investment-related fraud. FTC medians and IC3 means have different denominators and are not directly compared or pooled.

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

Cross-source agreement was defined before comparison as: (a) a positive age-severity gradient in both systems, and (b) identification of investment fraud as the highest-severity major fraud category. The comparison is pattern triangulation rather than statistical replication because microdata and variances are unavailable.

### 3.3. Research Ethics

Both sources are aggregate federal statistics containing no personal identifiers or individual records. The analysis does not constitute human-subjects research and presents no re-identification risk. Ethical attention remains necessary in interpretation. The paper avoids framing older adults as inherently gullible and attributes fraud to offender strategy and institutional context. It also avoids treating reported complaint statistics as population prevalence.

## 4.0. RESULTS

### 4.1. Age Gradient in the IC3 Data

Among the 419,766 IC3 complaints containing age information, total reported loss was $8.179 billion. Mean loss rose monotonically from $2,240 among complainants under 20 to $33,915 among those over 60 (Table 1).

Table 1: IC3 Complaints and Reported Loss by Age, 2023

| AGE | COMPLAINTS | COMPLAINTS % | LOSS | LOSS % | MEAN |
|---|---|---|---|---|---|
| Under 20 | 18,174 | 4.3 | $40.7M | 0.5 | $2,240 |
| 20–29 | 62,410 | 14.9 | $360.7M | 4.4 | $5,780 |
| 30–39 | 88,138 | 21.0 | $1.167B | 14.3 | $13,242 |
| 40–49 | 84,052 | 20.0 | $1.501B | 18.4 | $17,861 |
| 50–59 | 65,924 | 15.7 | $1.682B | 20.6 | $25,512 |
| Over 60 | 101,068 | 24.1 | $3.428B | 41.9 | $33,915 |

*Note:* Age was missing from approximately half of IC3 complaints. Means are aggregate loss divided by complaint count. Data from Federal Bureau of Investigation (2024, pp. 5–6); shares and means derived by the authors (see Appendix A).

Adults over 60 produced 24.1% of age-identified complaints and 41.9% of associated losses. Within this group, 5,920 complainants, or 5.9%, reported losing more than $100,000. The pattern shows disproportionate consequence, although aggregate data cannot determine whether the cause is assets, scheme type, targeting, reporting thresholds, or another mechanism.

### 4.2. Divergence Between Reported Prevalence and Severity

Tech-support fraud had the highest reported prevalence among over-60 categories, accounting for 17.5% of complaints and 17.2% of losses. Investment fraud accounted for 6.4% of complaints but 36.3% of losses (Table 2).

Table 2: Selected IC3 Fraud Categories for Complainants Over 60, 2023

| CATEGORY | COMPLAINTS | COMPLAINTS % | LOSS | LOSS % | MEAN |
|---|---|---|---|---|---|
| Tech support | 17,696 | 17.5 | $589.8M | 17.2 | $33,327 |

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

| CATEGORY | COMPLAINTS | COMPLAINTS % | LOSS | LOSS % | MEAN |
|---|---|---|---|---|---|
| Personal data breach | 7,333 | 7.3 | $109.7M | 3.2 | $14,963 |
| Confidence/romance | 6,740 | 6.7 | $356.9M | 10.4 | $52,951 |
| Non-payment/ delivery | 6,693 | 6.6 | $59.0M | 1.7 | $8,818 |
| Investment | 6,443 | 6.4 | $1.243B | 36.3 | $192,924 |
| BEC | 3,080 | 3.0 | $382.4M | 11.2 | $124,147 |
| Government impersonation | 3,517 | 3.5 | $179.6M | 5.2 | $51,079 |

*Note.* BEC = business email compromise. Percentages use 101,068 complaints and $3.428 billion in over-60 loss. Data from Federal Bureau of Investigation (2024, pp. 7–8); percentages and means derived by the authors (see Appendix A).

The derived mean for investment fraud was $192,924 per complaint, 5.7 times the over-60 mean. Business email compromise had a mean of $124,147, while confidence or romance fraud had a mean of $52,951. Personal data breach, despite ranking second in complaint volume, had a mean of $14,963. Non-payment or non-delivery had a mean of $8,818. The five categories producing the most loss accounted for 80.3% of losses but 37.1% of complaints.

The practical implication is direct. Allocation based on complaint volume will prioritise common schemes. Allocation based on severity will prioritise categories capable of destroying retirement security, housing stability, and family finances.

### 4.3. Three-Year Changes

Investment-fraud complaints rose from 2,104 in 2021 to 6,443 in 2023, a 206.2% increase, while reported loss increased 419.1%, from $239.5 million to $1.243 billion. Cryptocurrency-designated complaints rose 232.1% and losses rose 585.7% (Table 3).

Table 3: Selected IC3 Changes Among Complainants Over 60, 2021–2023

| CATEGORY | COUNT 2021 | COUNT 2023 | COUNT Δ | MEAN 2021 | MEAN 2023 | MEAN Δ |
|---|---|---|---|---|---|---|
| Investment | 2,104 | 6,443 | +206.2% | $113,819 | $192,924 | +69.5% |
| Crypto descriptor | 5,109 | 16,968 | +232.1% | $47,200 | $97,447 | +106.5% |
| Tech support | 13,900 | 17,696 | +27.3% | $17,117 | $33,327 | +94.7% |
| Government imposter | 3,319 | 3,517 | +6.0% | $20,846 | $51,079 | +145.0% |
| Identity theft | 8,902 | 3,010 | −66.2% | $6,630 | $11,479 | +73.1% |

*Note*. Cryptocurrency is a descriptor applied alongside a primary crime type. Data from Federal Bureau of Investigation (2024, pp. 9–10); means and percentage changes derived by the authors (see Appendix A).

Several categories showed severity intensification without equivalent volume growth. Government-imper-

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

sonation complaints increased 6.0%, while mean loss rose 145.0%, from $20,846 to $51,079. Tech-support complaints rose 27.3%, while mean loss rose 94.7%. Identity-theft complaints declined 66.2%, yet mean loss increased 73.1%.

This pattern demonstrates why count trends can mislead. Declining complaints do not necessarily mean declining burden. The limitation is particularly important for identity theft, where administrative remediation burden may exceed the financial loss captured in the report.

### 4.4. Limited Aggregate Reach of Financial Recovery

The IC3 Recovery Asset Team initiated its Financial Fraud Kill Chain in 626 incidents involving adults over 60. Those incidents represented $58.18 million in reported losses, of which $32.08 million was frozen (Table 4). Freezing places a hold on funds at the receiving institution; it is not the same as return of funds to the complainant, and this analysis does not measure how much frozen money was ultimately returned.

Table 4: IC3 Recovery Asset Team Coverage for Complainants Over 60, 2023

| MEASURE | VALUE |
|---|---|
| All complaints | 101,068 |
| All reported loss | $3,427,717,654 |
| FFKC incidents | 626 |
| FFKC share of complaints | 0.62% |
| Loss in FFKC incidents | $58,176,605 |
| Funds frozen | $32,079,603 |
| Frozen share of reported dollar value in FFKC incidents | 55.1% |
| Frozen share of all loss | 0.94% |

Note. FFKC = Financial Fraud Kill Chain. Data from Federal Bureau of Investigation (2024, pp. 5, 13). The freeze rate is funds frozen ÷ reported loss in FFKC incidents; coverage is funds frozen ÷ all reported over-60 loss. Frozen funds are not necessarily returned funds. Ratios derived by the authors (see Appendix A).

The 55.1% incident-level freeze rate, which is the share of reported dollar value in the 626 FFKC incidents that was frozen rather than a share of incidents or of funds returned, demonstrates effectiveness when eligibility and timing conditions are met. Yet the 626 incidents represented 0.62% of over-60 complaints, and frozen funds represented 0.94% of total reported over-60 losses. The mechanism is therefore effective within a narrow window but cannot serve as the general recovery pathway for the affected population. This conclusion concerns the FFKC only. Recovery through other channels, such as bank or card-issuer reversals, civil action, criminal restitution, or regulatory refunds, is not captured in the IC3 report, so the remaining 99.06% should not be read as the total unrecovered loss.

### 4.5. FTC Cross-Source Triangulation

FTC Sentinel data reproduce the age-severity pattern while separating likelihood of loss from magnitude conditional on loss (Table 5).

Table 5: FTC Loss Incidence and Median Loss by Selected Age Group, 2023

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

| AGE | REPORTS INDICATING LOSS | MEDIAN LOSS |
|---|---|---|
| 20–29 | 44% | $480 |
| 70–79 | 25% | $803 |
| 80 and older | 22% | $1,450 |

*Note*. Percentages describe the share of fraud reports in each age group indicating monetary loss. Medians are conditional on a reported loss. Data from Federal Trade Commission (2024, pp. 4, 13); values as published.

Adults aged 20 to 29 reported losing money in 44% of fraud reports. The proportion fell to 25% among adults aged 70 to 79 and 22% among adults aged 80 and older. Conditional on loss, however, the median rose from $480 among adults aged 20 to 29 to $803 among adults aged 70 to 79 and $1,450 among adults aged 80 and older.

This finding refines the meaning of vulnerability. The oldest reporters were less likely to indicate monetary loss, but their typical loss, once money was lost, was substantially greater. FTC data therefore support vulnerability of consequence rather than generalised vulnerability to deception.

The second cross-source convergence concerns investment fraud. FTC recorded more than $4 billion in investment-related loss and a median of $7,768, the highest median among the ten largest fraud categories. IC3 also ranked investment fraud first by loss among adults over 60, at $1.243 billion and a derived mean of $192,924. The amounts are not directly comparable because the systems use different taxonomies, denominators, truncation rules, and loss statistics. The rank-order agreement is nevertheless strong.

FTC data also show why IC3 means should not be treated as typical loss. Across all FTC fraud reports, aggregate reported loss exceeded $10 billion, but the median was $500. The gap is consistent with a highly right-skewed distribution in which a minority of reports account for catastrophic losses. IC3 severity ratios are therefore burden measures, while FTC medians are measures of the central experience among reports indicating loss.

### 4.6. Administrative Invisibility of Psychosocial Harm

The two published reports tabulate financial loss, category, and reporting characteristics (Federal Bureau of Investigation, 2024, pp. 5–16; Federal Trade Commission, 2024, pp. 4–16). Neither report tabulates psychological distress, family conflict, housing consequence, social withdrawal, health outcome, support referral, or service receipt. Because intake forms and data dictionaries were not examined, this finding concerns what is reported, not what is collected: the agencies may capture such information, for example in free-text complaint narratives, without publishing it.

The IC3 report itself acknowledges this missing domain. Its narrative (Federal Bureau of Investigation, 2024, pp. 14–16) describes adults over 60 who remortgaged or lost homes, emptied retirement accounts, borrowed from relatives, and in some cases died by suicide following shame or loss of sustainable income. The same report urges people not to feel afraid or embarrassed about reporting (Federal Bureau of Investigation, 2024, p. 3). Severe non-financial harm and barriers to disclosure are therefore recognised narratively while remaining absent from the published statistical tables.

The omission has institutional consequences. National statistics define the visible problem as a monetary

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

event. Financial and legal actors are then mobilised, while professions responsible for grief, trauma, material hardship, family functioning, and social participation remain peripheral.

## 5.0 DISCUSSION

### 5.1. Cross-Source Confirmation and Vulnerability of Consequence

The central contribution is the distinction between likelihood of reported loss and severity conditional on loss. IC3 establishes a monotonic increase in mean loss across age groups. FTC, a separately administered system, confirms the direction using medians while showing that older adults report a lower probability of losing money. Convergence across different intake systems and different statistics reduces the likelihood that the age-severity gradient is solely an artefact of one agency's classification or a few extreme cases.

This framing avoids two errors. The first is denial of disproportionate harm. Older adults plainly account for a much larger share of loss than complaint volume. The second is ageist overgeneralisation. The FTC evidence does not support the proposition that older people are more likely to lose money in a reported fraud encounter. Protective practice should therefore be justified by consequence, recoverability, and reduced economic recovery horizon, not by presumed incompetence.

### 5.2. Financial Recovery Is Necessary but Insufficient

The Recovery Asset Team finding clarifies the architecture of unmet need. The mechanism performs well in eligible, rapidly reported cases, freezing more than half of the reported dollar value in eligible incidents. But frozen funds equal under one percent of total reported loss. For most reported loss, the published data show no FFKC freeze, and recovery through other channels is not reported.

The finding should not be interpreted as operational failure. It demonstrates a scope limitation. Financial recovery requires speed, traceable transfers, and reachable accounts. When those conditions are absent, some other form of response is required. The published national reports do not show whether that response occurs.

This gap is precisely where a social work role becomes empirically defensible. The argument is not that social workers can replace investigators, banks, or regulators. It is that after their remedies are exhausted, material, psychological, relational, and administrative needs remain.

### 5.3. Severity-Informed Prevention

Prevention resources should consider both frequency and consequence. Tech-support fraud deserves substantial attention because it is common and costly. Investment fraud deserves disproportionate attention because a relatively small number of cases account for more than one-third of over-60 loss. Relationship-based investment schemes are especially important because their persuasive process develops over time and disables consultation.

Prevention should teach mechanisms rather than rapidly expiring scam lists. Manufactured urgency, requested secrecy, movement to encrypted channels, emotional escalation, guaranteed-return claims, and demands for irreversible payment recur across changing fraud narratives. Programmes should also establish a specific verification practice: before an unplanned transfer or disclosure prompted by incoming contact, pause, verify through an independently obtained channel, and consult a designated trusted person.

### 5.4. A Social Work Response Framework

A five-stage model follows from the findings.

- **Digital risk and consequence assessment.** Routine assessment should include online financial activity, recent unsolicited contact, new online re-

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

lationships involving money, prior victimisation, recent bereavement, social isolation, financial strain, and the presence of a trusted consultation partner. Questions should be framed as universal precautions to avoid undermining autonomy.

- **Mechanism-based education.** Community programmes should focus on persuasion structure and verification habits. Education should pre-empt shame by locating responsibility in organised offender practice rather than personal deficiency.
- **Crisis response.** Following disclosure, practitioners should assess immediate material need, housing risk, suicidal ideation, ongoing offender contact, and continued account exposure. Prompt connection to financial institutions and reporting bodies remains essential because recoverability declines with time.
- **Multidomain recovery.** Case management should integrate debt and benefit navigation, credit remediation, legal referral, grief or trauma support, and family mediation. Romance-fraud intervention should avoid humiliating confrontation, which may strengthen concealment and attachment.
- **Digital and social reintegration.** Permanent withdrawal from digital services can deepen isolation and reduce access to benefits and healthcare. Recovery should support safe re-engagement, renewed social participation, and, when desired, peer education.

### 5.5. Implications for Data-System Design

National fraud systems should retain their investigative purpose while adding a minimal psychosocial module or, where such information is already collected, publishing a tabulation of it. Three brief fields would transform the evidence base: whether the incident affected housing or essential expenditure, whether the complainant requested psychosocial or practical support, and whether a referral was offered. Optional distress screening and consent-based referral could be considered where crisis protocols are available.

These additions would not establish clinical outcomes, but they would quantify unmet need and create an accountable handoff between reporting and support. Without such fields, the systems will continue to count losses while remaining unable to describe what happens to the people who sustain them.

### 5.6. Implications for Social Work Education and Policy

Social work curricula should incorporate digital victimisation into human behaviour, practice, policy, and field education. Required competence is functional rather than forensic: recognising persuasion-based exploitation, conducting shame-sensitive inquiry, preserving self-determination, navigating reporting and remediation, and coordinating financial, legal, and clinical systems.

Agency protocols should define what happens when cyber fraud is disclosed. At minimum, protocols should cover immediate safety and material assessment, time-sensitive financial steps, documentation, mandated-reporting obligations where applicable, and warm referral rather than provision of a list of telephone numbers.

Policy should review the exclusion of fraud victims from services and compensation structures designed around violent crime. The absence of physical force does not imply absence of trauma, housing harm, or suicide risk. Liability frameworks for authorised transfers induced by deception also warrant scrutiny because they frequently place the full burden on the party least able to detect sophisticated manipulation.

### 5.7. Strengths and Limitations

The study's primary strength is cross-source triangulation. IC3 supplies detailed over-60 categories and recovery statistics; FTC supplies medians and separates loss incidence from loss severity. Their con-

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

vergence supports a more precise interpretation than either source permits alone. The study also derives burden indicators transparently and distinguishes measures that cannot be compared directly.

Several limitations remain. Both systems contain self-selected, unverified reports rather than survey estimates. Reporting is influenced by awareness, stigma, expected benefit, loss size, and contributor practices. The systems may share reports, so totals cannot be added and the sources are not statistically independent. Missing age data are substantial in IC3. FTC loss calculations exclude reports above $999,999, while IC3 applies different procedures, creating additional non-equivalence.

Aggregate data prevent assessment of dispersion, intersectional differences, repeat reporters, multivariate predictors, causal mechanisms, and individual recovery trajectories. Mean IC3 losses are influenced by extreme cases. FTC medians improve robustness but do not provide complete distributions. State-level variation cannot be interpreted without population age structure, wealth, and reporting propensity.

Both systems are United States sources and reflect the same national financial and legal environment. Cybercrime classifications and enforcement narratives differ materially in other settings, including Nigeria, where socioeconomic and institutional context shapes offending and official interpretation (Ibrahim, 2016; Lazarus & Okolorie, 2019). Cross-agency convergence is not cross-national replication. Finally, the central psychosocial outcomes remain absent. The study establishes their absence from published national statistics but cannot estimate their prevalence or test the effectiveness of social work intervention.

### 5.8. Future Research

The next phase should combine three designs. First, linkage or access to de-identified individual-level administrative records would permit median, percentile, and regression analysis, separating age, scheme type, payment method, and loss magnitude. Second, a qualitative critical-incident study with practitioners in ageing services, healthcare, housing, and income support should examine how fraud enters casework and where referral pathways fail. Third, a prospective victim study should measure distress, grief, family conflict, housing consequence, service use, and digital withdrawal over time.

A comparative study of victim-authored public narratives and institutional guidance could also specify which harms institutions recognise. Such work requires strict internet-research ethics, including attention to contextual privacy and avoidance of searchable verbatim quotation (franzke et al., 2020; Markham, 2012).

## 6.0. CONCLUSION

Two separately administered national reporting systems converge on a precise conclusion. Older adults are not necessarily more likely to report losing money to fraud, but when loss occurs the consequence is substantially greater. In IC3, adults over 60 comprise 24.1% of age-identified complaints and 41.9% of losses. In FTC Sentinel, the proportion of reports involving monetary loss falls with age, while the median rises to $1,450 among adults 80 and older. This is vulnerability of consequence, not evidence of generalised gullibility.

Investment fraud is the clearest high-severity category across both sources. Its burden cannot be addressed adequately through generic awareness messages. Financial recovery remains crucial, but funds frozen through the IC3 Financial Fraud Kill Chain equalled less than one percent of total reported over-60 loss value. For the remainder, the published record shows the event documented, no FFKC freeze, and the non-financial aftermath untabulated.

The central policy problem is therefore not only fraud incidence. It is the absence of a standardised response after financial remedies end. Social work has the

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

relevant competencies: assessment of social vulnerability, crisis intervention, grief and trauma support, family mediation, benefits and debt navigation, advocacy across fragmented systems, and construction of relational guardianship.

Protecting vulnerable populations from cyber fraud requires more than teaching individuals to recognise deception. It requires systems that measure the whole harm, preserve autonomy, respond without blame, and remain engaged when recovery of money is no longer possible. That is the emerging role this study identifies for social workers.

## REFERENCES

Bowker, G. C., & Star, S. L. (1999). Sorting things out: Classification and its consequences. MIT Press. https://doi.org/10.7551/mitpress/6352.001.0001

Boyle, P. A., Yu, L., Wilson, R. S., Gamble, K., Buchman, A. S., & Bennett, D. A. (2012). Poor decision making is a consequence of cognitive decline among older persons without Alzheimer's disease or mild cognitive impairment. PLOS ONE, 7(8), Article e43647. https://doi.org/10.1371/journal.pone.0043647

Bronfenbrenner, U. (1979). The ecology of human development: Experiments by nature and design. Harvard University Press.

Buchanan, T., & Whitty, M. T. (2013). The online dating romance scam: Causes and consequences of victimhood. Psychology, Crime & Law, 20(3), 261–283. https://doi.org/10.1080/1068316X.2013.772180

Burnes, D., Henderson, C. R., Jr., Sheppard, C., Zhao, R., Pillemer, K., & Lachs, M. S. (2017). Prevalence of financial fraud and scams among older adults in the United States: A systematic review and meta-analysis. American Journal of Public Health, 107(8), e13–e21. https://doi.org/10.2105/AJPH.2017.303821

Button, M., & Cross, C. (2017). Cyber frauds, scams and their victims. Routledge. https://doi.org/10.4324/9781315679877

Button, M., Lewis, C., & Tapley, J. (2012). Not a victimless crime: The impact of fraud on individual victims and their families. Security Journal, 27(1), 36–54. https://doi.org/10.1057/sj.2012.11

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608. https://doi.org/10.2307/2094589

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. International Review of Victimology, 21(2), 187–204. https://doi.org/10.1177/0269758015571471

Cross, C. (2018). Expectations vs reality: Responding to online fraud across the fraud justice network. International Journal of Law, Crime and Justice, 55, 1–12. https://doi.org/10.1016/j.ijlcj.2018.08.001

Cross, C. (2022). Using artificial intelligence (AI) and deepfakes to deceive victims: The need to rethink current romance fraud prevention messaging. Crime Prevention and Community Safety, 24(1), 30–41. https://doi.org/10.1057/s41300-021-00134-w

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud (Trends & Issues in Crime and Criminal Justice No. 518). Australian Institute of Criminology. https://doi.org/10.52922/ti148355

DeLiema, M., Deevy, M., Lusardi, A., & Mitchell, O. S. (2018). Financial fraud among older Americans: Evidence and implications. The Journals

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

of Gerontology: Series B, 75(4), 861–868. https://doi.org/10.1093/geronb/gby151

Federal Bureau of Investigation. (2024). 2023 elder fraud report. Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2023_IC3ElderFraudReport.pdf

Federal Trade Commission. (2024). Consumer Sentinel Network data book 2023. https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2023

Fischer, P., Lea, S. E. G., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. Journal of Applied Social Psychology, 43(10), 2060–2072. https://doi.org/10.1111/jasp.12158

franzke, a. s., Bechmann, A., Zimmer, M., Ess, C., & the Association of Internet Researchers. (2020). Internet research: Ethical guidelines 3.0. Association of Internet Researchers. https://aoir.org/reports/ethics3.pdf

Golladay, K., & Holtfreter, K. (2016). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. Victims & Offenders, 12(5), 741–760. https://doi.org/10.1080/15564886.2016.1177766

Hargittai, E. (2002). Second-level digital divide: Differences in people's online skills. First Monday, 7(4). https://doi.org/10.5210/fm.v7i4.942

Hazell, J. (2023). Spear phishing with large language models (arXiv:2305.06972). arXiv. https://doi.org/10.48550/arXiv.2305.06972

Helsper, E. J. (2012). A corresponding fields model for the links between social and digital exclusion. Communication Theory, 22(4), 403–426. https://doi.org/10.1111/j.1468-2885.2012.01416.x

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. International Journal of Law, Crime and Justice, 47, 44–57. https://doi.org/10.1016/j.ijlcj.2016.07.002

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. International Journal of Cyber Criminology, 10(1), 79–91. https://doi.org/10.5281/zenodo.58523

Judges, R. A., Gallant, S. N., Yang, L., & Lee, K. (2017). The role of cognition, personality, and trust in fraud victimization in older adults. Frontiers in Psychology, 8, Article 588. https://doi.org/10.3389/fpsyg.2017.00588

Kitchin, R. (2014). The data revolution: Big data, open data, data infrastructures and their consequences. Sage. https://doi.org/10.4135/9781473909472

Lazarus, S., & Okolorie, G. U. (2019). The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. Telematics and Informatics, 40, 14–26. https://doi.org/10.1016/j.tele.2019.04.009

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Lichtenberg, P. A. (2016). Financial exploitation, financial capacity, and Alzheimer's disease. American Psychologist, 71(4), 312–320. https://doi.org/10.1037/a0040192

Vol. 3. Issue 1.
ISSN: 3115-6940
EISSN: 3115-6932

Markham, A. (2012). Fabrication as ethical practice: Qualitative inquiry in ambiguous internet contexts. Information, Communication & Society, 15(3), 334–353. https://doi.org/10.1080/1369118X.2011.641993

Nicholson, J., Coventry, L., & Briggs, P. (2019). "If it's important it will be a headline": Cybersecurity information seeking in older adults. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (Paper 349, pp. 1–11). Association for Computing Machinery. https://doi.org/10.1145/3290605.3300579

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. Journal of Research in Crime and Delinquency, 50(2), 216–238. https://doi.org/10.1177/0022427811425539

Ross, M., Grossmann, I., & 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. https://doi.org/10.1177/1745691614535935

Scheerder, A., van Deursen, A., & van Dijk, J. (2017). Determinants of Internet skills, uses and outcomes. A systematic review of the second- and third-level digital divide. Telematics and Informatics, 34(8), 1607–1624. https://doi.org/10.1016/j.tele.2017.07.007

Smith, C. P., & Freyd, J. J. (2014). Institutional betrayal. American Psychologist, 69(6), 575–584. https://doi.org/10.1037/a0037564

van Dijk, J. (2020). The digital divide. Polity Press.

Wang, F., & Topalli, V. (2024). The cyber-industrialization of catfishing and romance fraud. Computers in Human Behavior, 154, Article 108133. https://doi.org/10.1016/j.chb.2023.108133

Whitty, M. T. (2013). The scammers persuasive techniques model. British Journal of Criminology, 53(4), 665–684. https://doi.org/10.1093/bjc/azt009

Whitty, M. T., & Buchanan, T. (2015). The online dating romance scam: The psychological impact on victims – both financial and non-financial. Criminology & Criminal Justice, 16(2), 176–194. https://doi.org/10.1177/1748895815603773

Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. European Journal of Criminology, 2(4), 407–427. https://doi.org/10.1177/147737080556056

INTERNATIONAL JOURNAL OF SOCIAL WORK AND DEVELOPMENT STUDIES

Department of Social Work

# International Journal of Social Work and Development Studies (IJSDS)

PUBLISHED BY PARAKLETUS PUBLISHING

CONTACT THE UNIVERSITY @
dsw@ust.edu.ng