# PROTECT VULNERABLE ADULTS FROM FINANCIAL EXPLOITATION ACT REPORT FY 2025

KANSAS
DEPARTMENT
OF INSURANCE

Vicki Schmidt, Commissioner
insurance.kansas.gov

# TABLE OF CONTENTS

# INTRODUCTION

## What is Financial Exploitation?

Financial exploitation is the illegal or improper use of an older or vulnerable adult's money, property, or resources for someone else's benefit. It can occur when another person or organization uses deception, intimidation, coercion, or undue influence to take or control an individual's assets. It may also involve the misuse of legal authority, such as power of attorney, guardianship, or trust, or taking property without permission when the adult cannot fully understand or consent. In short, financial exploitation happens when someone takes advantage of an older or vulnerable adult's finances for their own gain rather than for the adult's well-being.

## About the Protect Vulnerable Adults from Financial Exploitation Act

Beginning July 1, 2024, investment advisers and broker-dealers registered in Kansas are required to report suspected financial exploitation of older or vulnerable adults.

If an agent, investment adviser representative, or employee in a supervisory, compliance, or legal role reasonably suspects that an elder or vulnerable adult is being financially exploited, the firm has an obligation to report.

The firm must report the suspected financial exploitation to both the Compliance, Enforcement, and Anti-Fraud Division of the Kansas Department of Insurance (KDOI) and to Kansas Adult Protective Services (APS), a division of the Department of Children and Families.

The firm may delay a transaction or disbursement if there is reasonable belief that it may contribute to the financial exploitation of an elder or vulnerable adult. If a delay occurs, the firm must immediately report both the suspected exploitation and the reason for the delay.

For more details, refer to K.S.A. 39-1445, 21-5417. Questions may be directed to the Department's Compliance, Enforcement, and Anti-Fraud Division at (785) 296-5203.

# ATTEMPTED LOSS VS. ACTUAL LOSS

## About Attempted Loss

When a firm suspects that a vulnerable adult may be the target of financial exploitation, they are required to report the situation to KDOI and APS. After reporting, the firm may delay a transaction to give the client time to reconsider or verify the activity.

**Attempted Loss –** This refers to the amount of money that firms, KDOI, and APS are able to protect by stopping or delaying suspicious transactions before the funds are stolen.

## About Actual Loss

**Actual Loss –** The amount of money or assets that were successfully stolen by the fraudster often before the situation was reported to KDOI or APS.

## Loss Data

| | |
|---|---|
| **TOTAL ATTEMPTED LOSS:** | $4,973,572.90 |
| **TOTAL ACTUAL LOSS:** | $10,500,809.62 |
| **TOTAL COMBINED LOSS:** | $15,474,382.52 |

## About Delays

**Delay –** A delay means to halt money going out to give time for an investigation. The delay is initiated by the investment adviser or broker-dealer.

| | |
|---|---|
| **DELAYED CASES:** | 16 |
| **DELAYED AMOUNT:** | $1,741,073.83 |
| **TOTAL REPORTS:** | 140 |

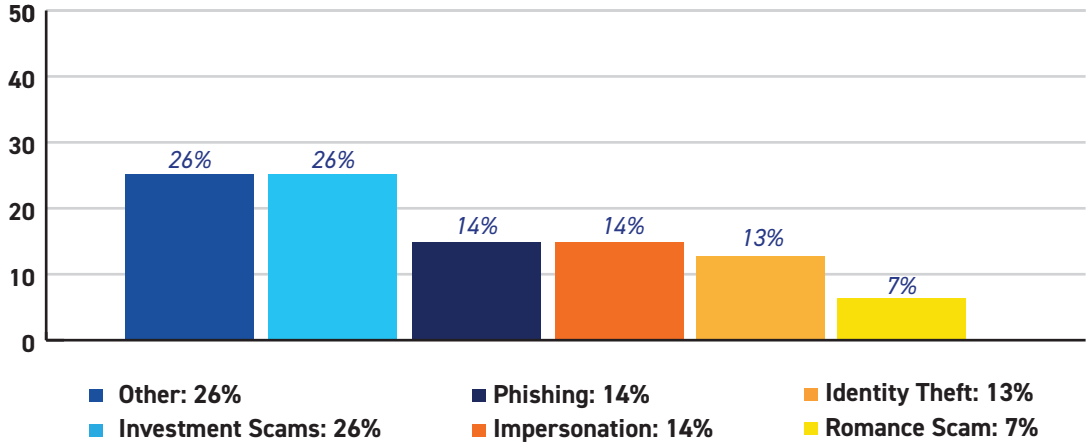
**Total Actual Lost + Total Attempted Loss**

# $15.4 MILLION

# FY 2025 DEMOGRAPHIC OVERVIEW

*Demographic overview of cases of financial exploitation of vulnerable adults, reported to the Kansas Department of Insurance*

## Top Scams




Female: 63 Male: 54

**Gender Breakdown of 140 Reports**

**Average Age**

**73**

**YEARS OLD**

**34/105**

**Counties in Kansas Reported Fraud**

# FY 2025 COUNTY OVERVIEW

## Attempted loss amount in each county from fiscal year 2025

| | |
|---|---|
| Barton | $5,700.00 |
| Butler | $65,151.32 |
| Cowley | $3,200.00 |
| Crawford | $75,000.00 |
| Douglas | $88,800.00 |
| Ellis | $7,000.00 |

| | |
|---|---|
| Geary | $190,000.00 |
| Grant | $4,789.99 |
| Johnson | $1,162,499.60 |
| Leavenworth | $105,000.00 |
| Marion | $75,000.00 |
| Marshall | $2,000.00 |

| | |
|---|---|
| Nemaha | $5,000.00 |
| Sedgwick | $425,390.85 |
| Shawnee | $881,160.00 |
| Washington | $3,665.11 |
| Wyandotte | $1,874,216.03 |
| **Total** | **$4,973,572.90** |

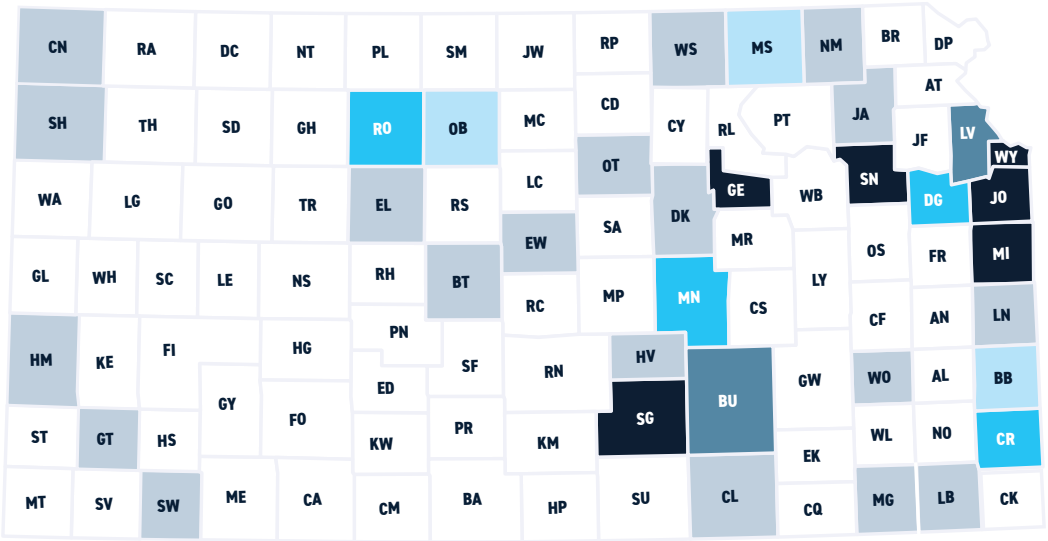
## Actual loss amount in each county from fiscal year 2025

| | |
|---|---|
| Barton | $17,367.29 |
| Bourbon | $67,500.00 |
| Butler | $173,473.28 |
| Cheyenne | $48,900.00 |
| Cowley | $10,800.00 |
| Crawford | $73,756.33 |
| Dickinson | $10,145.90 |
| Douglas | $58,933.97 |
| Ellis | $30,000.00 |
| Ellsworth | $500.26 |
| Geary | $60,000.00 |
| Grant | $516.01 |

| | |
|---|---|
| Hamilton | $2,000.00 |
| Harvey | $184.00 |
| Jackson | $294.96 |
| Johnson | $3,666,567.56 |
| Labette | $53.63 |
| Leavenworth | $143,712.05 |
| Linn | $3,450.00 |
| Marion | $75,000.00 |
| Marshall | $52,000.00 |
| Miami | $448,840.80 |
| Montgomery | $7,000.00 |
| Nemaha | $12,449.30 |

| | |
|---|---|
| Osborne | $60,000.00 |
| Ottawa | $1,003.86 |
| Rooks | $116,000.00 |
| Sedgwick | $2,567,058.01 |
| Seward | $540.38 |
| Shawnee | $1,741,449.68 |
| Sherman | $6,771.00 |
| Washington | $250.52 |
| Woodson | $7,917.83 |
| Wyandotte | $1,036,373.00 |
| **Total** | **$10,500,809.62** |

## Total attempted + actual loss across Kansas by county




**Total Actual + Attempted Loss**

- $0
- $50 - $50K
- $51K - $100K
- $101K - $150K
- $151K - 200K
- $201K - $250K
- $250K+

**Data shown reflects only counties with reported financial exploitation amounts. The absence of data for other counties does not indicate that no incidents of financial exploitation occurred.*

# TYPES OF SCAMS

**Advanced Fee –** An advanced fee scam occurs when a fraudster promises a large reward, but requires payment upfront, often disguised as taxes, legal costs, or processing fees prior to collection. Once the payment is made, no reward is delivered, and victims may be pressured to pay multiple times under the pretense of "unlocking" the promised reward.

**Affinity Fraud –** An advanced type of fraud that occurs through trust within a specific community, often targeting members based on shared characteristics and values such as religion, ethnicity or profession. The scammer often leverages trust within the group to defraud the members.

**Employment Scam –** An employment scam is a type of fraud where scammers advertise fake job opportunities to trick people into giving money or personal information. Victims are often asked to pay for training, background checks, equipment, or other "startup" costs, or to provide sensitive information such as Social Security numbers or banking details.

**Family Fraud –** Family fraud occurs when a family member takes advantage of another relative for financial gain, either knowingly or unknowingly. This can include convincing a relative to invest in a fake or risky business opportunity, or gaining access to financial accounts or other assets, and withdrawing funds without proper authorization. Because the fraud involves trust between family members, it can be difficult to detect and often causes financial loss and lasting emotional strain within the family.

**Identity Fraud –** Identity fraud occurs when scammers obtain personal information such as Social Security numbers, birth dates, or financial account details, and use it to commit financial crimes. This can include opening credit cards or personal loans, making purchases in the victim's name, taking a lien on the victim's home, or opening bank accounts for money laundering attempts. Often, the victim doesn't realize the fraud until significant damage has been done, including ruined credit, legal complications, or financial loss. Identity fraud is often combined with other scams, such as phishing or impersonation scams, to gain sensitive information more easily.

**Impersonation –** Impersonation schemes occur when a fraudster pretends to be a legitimate organization, such as a bank, tech company, government agency, or well-known service, such as PayPal or Microsoft. The scammer contacts the victim through a call, text, email, or social media, claiming there is an urgent problem with the victim's account or service requiring immediate action. The scammer seeks to gain the victim's personal information or demands repayment of funds sent to the victim in error by the organization.

**Inheritance –** Inheritance fraud occurs when scammers contact victims claiming they are entitled to a large inheritance from a distant relative or unknown benefactor. To access the funds, the victim is asked to pay fees for taxes, legal processing, or administrative costs. These schemes often use official-looking documents, emails, or calls impersonating lawyers processing the will of the alleged relative.

**Investment Fraud –** Investment fraud occurs when scammers offer fake or misleading opportunities that promise high returns with little or no risk. Victims may be encouraged to invest in stocks, cryptocurrency, real estate, or other ventures that don't exist or are manipulated. Scammers often use professional-looking documents, fabricated success stories, official-looking websites, or social media groups with fictitious members to encourage larger investments. The alleged funds are held by the scammers and require fees or taxes to be paid upfront prior to being released. Once these fees have been paid, the scammer will fabricate continual financial requirements or investment losses to deny payout to the victim.

# TYPES OF SCAMS

**Recovery Fraud –** Recovery Fraud is a scheme that targets individuals who have already lost money, promising to help them recover their funds for a fee. Scammers may pose as lawyers, investigators, or consumer protection agencies to create credibility. They often claim they will track down lost funds or prosecute the fraudsters, but require payments for legal costs, taxes, or administrative fees. Once the victim has paid, the scammer will either vanish or require additional payments to continue the investigation.

**Phishing –** Phishing is a scheme where scammers send emails, text messages, or utilize fake websites designed to look like they come from trusted companies, such as banks or other payment services, digital software, or government agencies. Phishing schemes aim to collect personal information such as Social Security numbers, passwords, and credit card numbers. This information can be used to steal money, commit identity fraud, or gain unauthorized access to accounts. Phishing often relies on urgency or fear to pressure victims into responding quickly without questioning the legitimacy of the correspondence.

**Pig Butchering –** Pig butchering is a long-term scheme where scammers build trust with the victim, often through social media or dating apps. Once trust has been established, the scammer will gradually convince the victim to invest in a fake or manipulated investment or cryptocurrency platform. The scammer slowly encourages larger deposits, making it appear as though the investments are growing, until the victim has contributed a significant amount of money.

**Ponzi/Pyramid –** A Ponzi or pyramid scheme is an investment fraud that relies on funds from new participants to pay returns to earlier investors, creating the illusion of profitability. Due to the low or non-existent revenue being generated, the scheme inevitably collapses as recruitment slows, leaving most participants with losses.

**Romance -** Romance fraud is a scheme where scammers use online dating platforms, social media, or messaging apps to create fake identities and develop emotional relationships with the victim. Often, but not exclusively, using the identity of a celebrity or public figure. Over time, the scammer builds trust and manipulates the victim's feelings before fabricating emergencies or personal crises that require financial assistance. Victims may be asked for money repeatedly under different pretexts, and they can also request personal or financial information for exploitation later.

**Sweepstakes –** Sweepstakes fraud occurs when scammers falsely inform someone that they have won a prize, such as cash, a vacation, or a luxury item. To claim the prize, the victim is told they must first pay fees, often for taxes. These schemes often use official-looking letters, phone calls, or emails to appear legitimate, making victims believe they are dealing with a trusted organization.

785-296-3071
KDOI.@ks.gov
insurance.kansas.gov

KANSAS
DEPARTMENT
OF INSURANCE