



KinKeeper

RESEARCH WHITE PAPER

When the Pattern Changes

What transactions and property records can -
and cannot - reveal

Know what is normal.

Notice what changed.

Check it without taking over.

EVIDENCE CUTOFF

July 16, 2026

COMPANION COURSE

Money Safety & Monitoring Playbook

Research synthesis for education. Monitoring can surface changes; it cannot establish fraud or guarantee against loss.

Executive brief

The signal is usually the change, not the purchase

A \$900 transfer can be ordinary for one household and unprecedented for another. A new charity may reflect a deliberate gift. A missed utility payment may be a bank error, a move, a changed due date, a cash-flow problem, or a sign that managing bills has become harder. The transaction alone does not settle the question.

What deserves attention is often the change around it: a new recipient, an unfamiliar payment route, several transfers in quick succession, money moved from savings immediately before it leaves the account, an expected deposit that does not arrive, or an abrupt change in who controls statements and access. Federal guidance repeatedly treats activity that is unusual for the particular account holder as more informative than a universal rule about what an older person should buy.[7][8]

The useful question is not, “Was that a bad purchase?” It is, “What changed, what else changed with it, and is there a safe explanation?”

That approach protects two things at once. It gives families and institutions a better chance of recognizing fraud or exploitation, and it protects the older adult from having ordinary choices treated as evidence of incapacity.

Four findings should shape any monitoring plan

- 1. **Reported harm is large, but the numbers describe different systems.** In 2025, people age 60 and older filed 201,266 complaints with the FBI's Internet Crime Complaint Center and reported \$7.748 billion in losses. FinCEN separately identified roughly \$27 billion in elder-financial-exploitation-related suspicious activity in 155,415 Bank Secrecy Act filings during an earlier one-year period. These figures cannot be added: one reflects self-reported cybercrime complaints and the other suspicious activity reported by financial institutions.[1][2]
- 2. **A trusted person can be part of the risk.** FinCEN classified about four in five analyzed filings as scams involving strangers or imposters and about one in five as theft by a person who was otherwise trusted. In the theft-related filings, adult children were the most frequently identified perpetrators.[2]
- 3. **Financial-management changes can precede a diagnosis.** Newer longitudinal research links later memory-disorder diagnoses with earlier changes in payment delinquency, credit utilization, balances, and credit scores. The findings are meaningful at the population level, but they do not turn a late payment into a clinical test.[4][5][6]
- 4. **Monitoring is useful only when it leads to a proportionate response.** An unexplained risk score can create alarm or family conflict. A useful alert explains the change, shows the supporting facts, respects the account owner's sharing choices, and provides an official route to verify what happened.[7][10]

Current figures, kept in their proper lanes

Measure	Result	What it means
IC3 complaints from people age 60+ in 2025	201,266	Reports submitted to one federal cybercrime

Measure	Result	What it means
		complaint system
Reported IC3 losses for people age 60+ in 2025	\$7.748 billion	Reported loss, not a national prevalence estimate
IC3 complainants age 60+ reporting losses above \$100,000	12,444	High-loss reports within the IC3 dataset
FinCEN elder-financial-exploitation-related filings analyzed	155,415	Suspicious activity reports from financial institutions
Dollar value indicated in those FinCEN filings	About \$27 billion	Suspicious activity, not verified victim loss

Sources: FBI IC3 2025 Annual Report and FinCEN's 2024 trend analysis.[1][2]

Scope and definitions

Similar patterns can come from different problems

This report examines financial changes involving community-dwelling older adults and the people or institutions helping them. It focuses on everyday transaction activity, credit-management research, trusted contacts, known-person exploitation, and property-record monitoring. It does not evaluate investment suitability, diagnose a health condition, or provide legal advice.

Four categories can produce similar-looking account activity:

- 5. **Fraud or a scam.** A stranger or imposter persuades someone to send money, reveal access, or move funds for a promised benefit or false emergency.
- 6. **Financial exploitation.** A family member, caregiver, fiduciary, friend, professional, or other person improperly uses or controls someone else's money or property.
- 7. **A money-management change.** Bills may be missed, deposits overlooked, subscriptions duplicated, or fees accumulated without another person stealing the money.
- 8. **An ordinary life change.** Travel, repairs, gifts, health expenses, a move, helping family, a new hobby, or a changed payment schedule can make the account look different for legitimate reasons.

The categories can overlap. A scammer may gain remote access and take over an account. A trusted person may conceal withdrawals. A household may experience a genuine money-management problem and then become more vulnerable to a scam. The same visible signal can therefore require different responses.

What “baseline” means

A financial baseline is a working picture of what is typical for the person and account. It can include:

- normal transaction amounts and ranges;
- recurring income and bills;

- familiar merchants, charities, and recipients;
- ordinary ATM use and transfer frequency;
- usual payment channels, locations, and timing;
- the accounts that are active or rarely used;
- expected seasonal or annual events;
- who is authorized to help and what that help looks like.

A baseline is not a rule that freezes someone into past behavior. People change their minds and routines. It is a comparison point that makes a new event easier to explain.

How this paper was researched

KinKeeper conducted a narrative synthesis of sources available through July 16, 2026. Priority went to current federal regulators and law-enforcement reports, official consumer guidance, and peer-reviewed original research. Historical sources were used when they supplied a method or detail not available in newer reporting.

The synthesis keeps three evidence streams separate:

- **Complaint data:** what people reported to the FBI or FTC. These systems undercount harm, depend on awareness and access, and may contain incomplete or duplicated reports.
- **Suspicious activity reports:** what financial institutions flagged and reported under Bank Secrecy Act processes. Suspicion is not adjudication, and the reported amount is not automatically a victim's confirmed loss.
- **Clinical and credit research:** group-level associations between later diagnoses and earlier credit outcomes. These studies do not establish that any one transaction pattern diagnoses disease.

This is not a systematic review or meta-analysis. It does not estimate the sensitivity or specificity of consumer transaction-monitoring products, because the necessary independent outcome evidence is not yet available.

The reported scale

Losses are increasing faster than complaint counts in several datasets

The FBI's 2025 annual report recorded 201,266 complaints from people age 60 and older, 37% more than in 2024. Reported losses reached \$7.748 billion, a 59% increase. The report also recorded an average reported loss of \$38,500 and 12,444 complainants reporting losses above \$100,000.[1]

Investment fraud accounted for the largest reported loss among people age 60 and older in that dataset, followed by tech-support scams, confidence or romance fraud, business email compromise, and government impersonation. Cryptocurrency appeared as a descriptor in \$4.347 billion of reported losses for that age group. A descriptor can overlap with a crime category, so these values are not separate buckets to add together.[1]

FTC data tell a complementary story. Adults age 60 and older reported \$2.4 billion in fraud losses to the Consumer Sentinel Network in 2024, roughly four times the amount reported in 2020. Older adults

continued to report losing money at a lower rate than younger adults, but reported much higher median losses when a loss occurred. That distinction matters: the risk is not that older adults uniformly make poorer decisions. It is that some successful schemes produce unusually severe losses.[3]

In high-loss business and government impersonation reports, the FTC found that reports of losses above \$10,000 more than quadrupled from 2020 to 2024, while reports above \$100,000 rose nearly sevenfold. For losses above \$100,000, bank transfers were the most frequently reported payment method. The starting story often involved a fake security alert, business, or government agency telling the person that money was at risk.[17]

Suspicious activity data show both strangers and people who are known

FinCEN examined 155,415 Bank Secrecy Act filings submitted between June 15, 2022 and June 15, 2023. The filings indicated roughly \$27 billion in elder-financial-exploitation-related suspicious activity. About 80% involved scams, usually money transferred to a stranger or imposter for a benefit that never arrived. About 20% involved theft by a person who was otherwise trusted.[2]

The distinction changes what monitoring must notice. Stranger scams often produce a visible payment event: a wire, crypto purchase, transfer app, cashier's check, gift card, or rapid movement of funds. Known-person exploitation may look quieter: recurring ATM withdrawals, card use by another person, changed account ownership, missing statements, transfers to a relative, misuse of a power of attorney, or an unexpected deed change.[8][12][15]

No transaction engine can observe coercion, fear, isolation, or who is standing beside the account holder. That is why financial data should support, not replace, a human conversation.

What newer research says about financial change and cognition

Financial management is a complex daily task

Paying bills on time requires attention, memory, planning, arithmetic, judgment, and the ability to manage changing instructions. A difficulty in any one part of that process can appear in the financial record before it appears in a clinical record. It can also arise for reasons unrelated to cognitive decline, including illness, grief, depression, vision changes, technology changes, income pressure, or a simple administrative error.

The relevant research asks a narrow question: when a large group of people later receive a memory-disorder diagnosis, do their earlier credit outcomes differ from otherwise comparable people who do not receive that diagnosis?

The 2025 evidence is large and longitudinal

Gresenz and colleagues linked nationally representative credit-reporting data with Medicare records. The research followed nearly 2.5 million older adults over 17 years, including approximately 500,000 who were later diagnosed with Alzheimer's disease or a related dementia. The peer-reviewed paper reported effects years before diagnosis across payment delinquency, delinquent balances, credit utilization, mortgage outcomes, and credit scores.[4][5]

NIA's summary reported that missed credit-card payments began increasing about five years before diagnosis and mortgage-payment problems about three years before diagnosis. In the year before diagnosis, people in the later-diagnosed group were more than 34% more likely to miss a credit-card payment and 17% more likely to miss a mortgage payment than in earlier years.[4]

The effects were not uniform. They were larger for single people and Black individuals in parts of the analysis. That pattern may reflect differences in household support, resources, credit access, structural inequality, and timing of diagnosis as well as disease effects. It is a warning against building a single “normal” model for every household.[4][5]

An earlier JAMA Internal Medicine study also found small but statistically significant differences before diagnosis. Single Medicare beneficiaries later diagnosed with Alzheimer's disease or a related dementia were more likely to miss payments as early as six years before diagnosis and to develop subprime credit scores about two and a half years before diagnosis than demographically similar beneficiaries without the diagnosis.[6]

What the studies do not establish

The research does not show that a late bill proves cognitive decline. It does not validate a clinical score from a checking account. It does not show that family access to every transaction improves health or financial outcomes. The studies rely primarily on credit-report events, which omit cash spending, many bank-account transactions, fraud that is not reported to a lender, informal household arrangements, and the explanation behind the event.[4][5][6]

The appropriate inference is narrower:

A new, repeated difficulty managing bills can be worth discussing, especially when it appears alongside other changes. It is not a diagnosis and should not be used to remove a person's control.

If financial changes arrive with new memory concerns, confusion, difficulty completing familiar tasks, or another health change, the older adult can decide whether to discuss the pattern with a qualified clinician. A monitoring product should not make that referral automatically from transaction data alone.

A better model for spotting meaningful change

Baseline, change, context, corroboration

Four questions make an alert more useful and less intrusive.

9. **Baseline:** What is normal for this person, account, category, recipient, and time of month?
10. **Change:** What is new, missing, larger, faster, repeated, or out of sequence?
11. **Context:** Is there an ordinary explanation - travel, repairs, a gift, a move, health costs, a changed bill, or a planned purchase?
12. **Corroboration:** Do other signals point in the same direction?

The fourth question is where a pattern often becomes meaningful. A new payee alone may be routine. A new payee followed by repeated P2P transfers, a savings-to-checking transfer, and a rapid balance decline deserves a faster review. A missed pension deposit may be a processing delay. A missed deposit followed by overdraft fees and unpaid recurring bills shows a broader problem.

Signals gain meaning in combination

Signal	Alone	Stronger when combined with
First payment to a new recipient	Often ordinary	Large amount, repeated transfers, risky rail, secrecy or urgency
Wire, crypto, gift card, or P2P payment	Legitimate uses exist	New recipient, unusual amount, rapid repetition, account drain
Large purchase	May be planned	New merchant, out-of-pattern channel, unusual location, follow-on transfers
Missed expected bill	Could be an administrative error	Repetition, late fees, service interruption, other missed bills
Missing expected deposit	Could be timing or eligibility	Low balance, overdraft, changed deposit destination, repeated absence
Frequent ATM withdrawals	May reflect a new cash preference	Larger amounts, new locations, an accompanying person controlling access
Dormant account becomes active	Could be planned consolidation	New payee, rapid withdrawal, changed contact information
Property-record change	Could be authorized	Owner does not recognize it, unexpected loan contact, identity-theft indicators

Regulators give financial institutions similar examples. An unexpected large wire from an account with no comparable history is a reason to investigate, not because every wire is fraudulent, but because the account's own history makes the event unusual.[7]

What a household can monitor

Fast-moving payment patterns

Some payment routes deserve faster review because money can move quickly or recovery can be difficult. Current complaint data repeatedly identify bank transfers, cryptocurrency, cash, payment apps, gift cards, and wires in high-loss scams.[1][3][17]

Useful signals include:

- a first-time wire or unusually large transfer;
- cryptocurrency exchange or kiosk purchases outside the person's normal activity;
- a gift-card purchase followed by several more purchases;
- a new P2P recipient receiving repeated payments;
- savings moved into checking immediately before a large outflow;
- several payments made within hours or days under a new pattern;
- a rapid decline across more than one connected account.

The response should not be “crypto equals fraud” or “a new payee is prohibited.” It should be “this route and sequence are unusual; verify before more money moves.”

Slow leaks and missing events

Not every harmful pattern arrives as a dramatic transfer. A useful monitoring plan also looks for money that leaves gradually or fails to arrive:

- duplicate charges or duplicate bill payments;
- subscriptions that begin, increase, or continue after they are no longer wanted;
- repeated overdraft, late, or insufficient-funds fees;
- an expected Social Security, pension, annuity, or payroll deposit that does not appear;
- recurring bills that stop being paid;
- a low balance that follows a new pattern rather than one large event;
- repeated small test charges before larger unauthorized transactions.

These events are not necessarily exploitation. They may reveal a merchant issue, a benefit problem, a forgotten renewal, a cash-flow strain, or a task that has become harder to manage. The value is the earlier conversation.

Changes involving another person

Transaction data become especially limited when the concern involves someone the account holder knows. CFPB and DOJ guidance identify signs that may never appear in a merchant category:

- money or property is missing;
- another person prevents private conversations or controls decisions;
- statements stop arriving;
- names are added to accounts without a clear explanation;
- beneficiaries or ownership documents change unexpectedly;
- a new friend, caregiver, relative, or fiduciary begins handling money;
- cards, checks, powers of attorney, or property are used outside the authority granted.[8][12]

Families should be careful here. The person receiving an alert may also be the person misusing the money. Monitoring design therefore needs more than “notify the family.” It needs owner-controlled routing, the ability to choose more than one trusted channel, and a clear path to the financial institution or an outside professional.

Property records: useful notice, limited protection

A public-record change is a prompt to verify

Property can be the household's largest asset, yet it sits outside ordinary bank alerts. A property-monitoring service may compare current public records with a confirmed baseline and flag a change in ownership, deed, lien, mortgage, or related record when the available source changes.

That can be useful. It does not create a lock around the title. The FTC warns that services marketed as “home title locks” do not stop a fraudulent filing and are not title insurance. At most, monitoring may tell the owner after a record has changed.[13]

A responsible property alert should therefore say:

- which public field changed;
- which source reported the change;
- when the source was checked;
- whether other sources agree;
- that the change is not automatically fraud;
- how to contact the official recorder or another qualified professional.

It should not say that the home was “stolen,” that fraud was confirmed, or that monitoring prevented a transfer.

Property and transaction signals may corroborate one another

A property-record change becomes more concerning when it appears with an unexplained loan, large deposit followed by rapid withdrawals, a new person controlling mail, or identity-theft indicators. The combination can guide a faster review. It still cannot establish who authorized the filing or whether the legal record is valid.

Connection without takeover

A trusted contact is not a co-owner

Brokerage firms ask customers to consider naming a trusted contact. That person is similar to an emergency contact: the firm may reach them when it cannot contact the account owner or reasonably suspects exploitation. The trusted contact does not automatically gain authority to trade, make decisions, or view balances and transactions. Those powers require separate legal authorization.[10][16]

This limited role is a good model for family monitoring. The account owner can choose:

- which accounts or property records are monitored;
- whether a trusted person sees alerts only, summaries, or full details;
- which categories or merchants remain private;
- the threshold for sharing an alert;
- which person receives urgent versus routine notices;
- when access is paused or revoked.

The goal is not to give a family member a continuous view of someone's spending. It is to create a second channel for events the owner has decided deserve help.

Ask about the event, not the person's competence

An alert should open with observable facts:

“This transfer is new and larger than your usual transfers. Did you mean to send it?”

It should not open with an accusation:

“You are making bad decisions again.”

The first version invites context. The second creates shame, encourages secrecy, and turns the family relationship into a test of capacity.

Helpful family language includes:

- “I’m glad we caught this together.”
- “Is this expected, or should we call the bank?”
- “Would you like me to stay with you while you use the number on the statement?”
- “What do you want shared next time?”

What good monitoring should do

Explain the reason, not only the score

A useful alert answers five questions:

13. What happened?
14. What part is different from the baseline?
15. What other signals, if any, appeared with it?
16. How current and complete is the data?
17. What is the safest next verification step?

A score without those facts can create false confidence or unnecessary alarm. The account owner and trusted person need the evidence, not a machine's verdict.

Show quiet work and blind spots

Ongoing monitoring creates value even when nothing is flagged, but only if the user can see what was reviewed. A clear status can show:

- institutions and accounts connected;
- transaction history reviewed;
- recurring income and bills tracked;
- property records checked;
- the date and freshness of each source;
- disconnected accounts or permissions that need renewal;
- areas that are not covered.

“No change found” is different from “no current data.” A monitoring product should never blur the two.

Keep health inference outside the alert engine

The cognitive research supports education and careful planning. It does not support a consumer product declaring that someone has cognitive decline based on a transaction pattern. A responsible system may flag repeated missed payments, unusual fees, or a broad pattern break. It should describe those events in financial terms and leave health interpretation to the person and a qualified clinician.[4][5]

When a pattern deserves action

Pause, ask, verify, escalate

When an event may still be in progress:

18. **Pause additional action.** Do not send another payment, install software, read a code, or move money to a “safe” account while the event is being checked.
19. **Ask without accusation.** Confirm whether the account owner recognizes and intended the activity. If another person may be exerting pressure, create a private opportunity to speak.
20. **Verify through an official channel.** Use the number on the card, statement, official app, or institution website typed directly. Do not use a number or link supplied by the unexpected caller or message.
21. **Contact the institution quickly.** Ask about stopping, recalling, disputing, or securing the transaction or account. Available options depend on the payment type, timing, institution, and facts.
22. **Preserve records.** Save messages, receipts, transaction details, names, phone numbers, and dates. Do not continue engaging simply to gather more evidence.
23. **Escalate when appropriate.** Reporting routes may include local law enforcement, a state attorney general, Adult Protective Services, the FTC, IC3, or the National Elder Fraud Hotline. CFPB maintains a current guide to the appropriate channels.[14]

If the concern involves a brokerage account, the firm may have trusted-contact and temporary-hold procedures. If the concern involves property, contact the official recorder or land-record office and a qualified attorney or title professional appropriate to the situation.[7][16]

No response path guarantees recovery. Speed can preserve more options, especially before money moves through additional accounts.

A household framework: Know, notice, check

Know what is normal

List the accounts, expected deposits, recurring bills, ordinary transfer routes, important property records, and official contact methods that matter. The account owner decides what is included and who may help.

Notice what changed

Look for a change in amount, recipient, route, timing, frequency, location, account activity, expected income, bill payment, access, ownership, or property record. One signal is a question. Several related signals can create urgency.

Check another way

Leave the channel that produced the request or alert. Confirm with the account owner and the institution through an official route. Bring in the trusted person the account owner selected, not the person who simply demands access.

This framework does not require a household to monitor every purchase. It creates a repeatable response for the moments already defined as important.

Putting the research into practice

The companion *Money Safety & Monitoring Playbook* helps an older adult or family:

- identify the financial baseline that matters;
- recognize fast-moving and slow-moving patterns;
- distinguish an alert from a conclusion;
- choose a limited trusted contact;
- add a property-record check;
- save an official response plan.

The Playbook is practical and can be completed without connecting financial accounts. The research paper explains why those actions matter and where the evidence remains uncertain.

Where KinKeeper fits

KinKeeper Money Monitoring is designed to provide a second set of eyes across read-only financial activity and selected property records. It can compare current activity with a household's established patterns, explain why an event deserves attention, and route masked alerts according to the account owner's choices. KinKeeper cannot move money, determine whether someone has cognitive impairment, prevent a fraudulent property filing, or guarantee that a loss will be avoided.[18]

The product is one optional way to maintain the review routine described in this paper. A household can also use bank alerts, brokerage trusted contacts, official county record alerts, calendar reminders, and a written family plan.

Limitations and research gaps

This report has several limits.

- Complaint systems are affected by awareness, access, duplicate reporting, categorization, and underreporting. Their losses should not be interpreted as complete national totals.
- Suspicious activity reports describe concerns identified by institutions. They are not adjudicated findings, and the dollar amount can exceed confirmed victim loss.
- Credit studies observe outcomes reported to credit bureaus, not the full household ledger or the reason behind each event.
- Later diagnosis is not the same as symptom onset, and disparities in diagnosis timing can affect the measured pre-diagnosis period.
- Older adults are diverse in income, culture, household structure, health, financial experience, and preferred support. A baseline or model trained on one group may perform poorly for another.
- Independent evidence has not yet established how accurately consumer monitoring products reduce completed fraud, improve recovery, or avoid harmful false positives.

- Property-record availability, terminology, update cadence, and correction processes vary by jurisdiction.

The most important research gaps are product-level outcomes, false-positive burden, autonomy and privacy effects, performance across diverse households, and the ethics of using financial data for health-related inference.

Review notice

Evidence reviewed through July 16, 2026. Next scheduled review: October 16, 2026, or earlier if major fraud reporting, financial-regulatory guidance, cognitive research, or KinKeeper product availability changes.

References

1. Federal Bureau of Investigation, Internet Crime Complaint Center. 2025 IC3 Annual Report. 2026. Accessed July 16, 2026. Complaint reports and reported losses are not prevalence estimates.
2. Financial Crimes Enforcement Network. Elder Financial Exploitation: Threat Pattern & Trend Information, June 2022 to June 2023. April 18, 2024. Accessed July 16, 2026.
3. Federal Trade Commission. Protecting Older Consumers 2024-2025. December 2025. Accessed July 16, 2026.
4. National Institute on Aging. Difficulty Managing Bills May Signal Early Dementia. February 18, 2025. Accessed July 16, 2026.
5. Gresenz CR, Mitchell JM, Rodriguez B, Wang C, Turner RS, and van der Klaauw W. The Financial Consequences of Undiagnosed Memory Disorders. Journal of Financial Economics. October 2025;172:104-149.
6. Nicholas LH, Langa KM, Bynum JPW, and Hsu JW. Financial Presentation of Alzheimer Disease and Related Dementias. JAMA Internal Medicine. 2021;181(2):220-227.
7. Board of Governors of the Federal Reserve System, CFPB, FDIC, FinCEN, NCUA, OCC, and state financial regulators. Interagency Statement on Elder Financial Exploitation. December 4, 2024.
8. Consumer Financial Protection Bureau. How Can I Tell If a Friend, Neighbor, or Family Member Is a Victim of Financial Exploitation? Reviewed September 5, 2025.
9. Consumer Financial Protection Bureau. Protecting Older Adults from Fraud and Financial Exploitation. Updated March 10, 2026.
10. SEC Office of Investor Education and Advocacy, FINRA, and NASAA. Investor Bulletin: Why You Should Consider Adding a Trusted Contact to Your Account. August 25, 2025.
11. Financial Industry Regulatory Authority. Regulatory Notice 20-34: Retrospective Rule Review - Senior Investor Protection. October 6, 2020.
12. U.S. Department of Justice, Elder Justice Initiative. Financial Exploitation. Accessed July 16, 2026.
13. Federal Trade Commission. Home Title Lock Insurance? Not a Lock at All. August 27, 2024.
14. Consumer Financial Protection Bureau. I Think I or Someone I Know Was the Victim of a Scam or Financial Exploitation. Who Can I Contact for Help? Reviewed September 5, 2025.

-
15. Consumer Financial Protection Bureau. [Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends](#). February 27, 2019.
 16. Financial Industry Regulatory Authority. [Protecting Older Investors from Financial Exploitation](#). July 15, 2025.
 17. Federal Trade Commission. [False Alarm, Real Scam: How Scammers Are Stealing Older Adults' Life Savings](#). August 7, 2025.
 18. KinKeeper. Money Monitoring Product Expansion Brief. July 16, 2026. Internal product-context source; not used as evidence for external outcomes.