

Before the First Scam Call

How the personal-data economy helps scammers find, profile, and approach older adults – and which defenses are supported by evidence.

EVIDENCE CUTOFF

July 15, 2026

COMPANION COURSE

The Personal Data & Privacy Playbook

WELLBEING PRIVACY MONEY IDENTITY

Research synthesis for education. Data removal can reduce exposure; it cannot guarantee protection from fraud.



EXECUTIVE BRIEF

The scam often starts before the message arrives

Personal data does not cause fraud. It can, however, make a person easier to locate, classify, and approach. People-search sites can turn one identifier into a report containing age, addresses, property history, and family relationships. Commercial brokers can add purchasing behavior, interests, inferred traits, and response patterns.^{[1][2]}

This is not only a theoretical privacy problem. In the Epsilon criminal case, federal prosecutors showed that employees used models built on a database of 100 million U.S. households to identify likely responders and knowingly sold targeted lists to fraud operators. One client used those lists in a scheme that defrauded more than 218,000 people of more than \$23.7 million.^[3]

The practical response is layered. Remove high-value public listings, stop providing primary contact information to low-trust forms, strengthen critical accounts, and keep a consent-based family review routine. These steps reduce particular exposures. Research has not yet quantified how much broker removal changes scam attempts or financial loss.

The central finding

Privacy cleanup is best understood as exposure reduction, not a force field. It gives unknown senders less accessible information while account security and independent verification protect against different failure points.

01

Direct evidence

Modeled consumer lists have been knowingly sold to operators of elder-fraud schemes.

02

Defensible action

Current listings can be removed, important accounts hardened, and future sharing reduced.

03

Open question

The effect of broker removal on fraud incidence and loss has not been adequately measured.



READ THE CLAIMS AT THE RIGHT STRENGTH

A useful defense starts by separating proof from inference

Privacy conversations often jump from 'this information is available' to 'removing it prevents fraud.' The first statement is observable. The second requires outcome evidence that the field does not yet have. This paper uses three evidence grades so practical guidance does not borrow more certainty than the research can support.

ESTABLISHED

Data is collected, combined, inferred, sold, and sometimes used to select fraud targets. Account authentication can reduce takeover risk.

STRONG INFERENCE

Less exposed information can make routine discovery and personalization harder through the channels that were cleaned.

UNSETTLED

No credible population estimate shows how much data removal changes scam contact, completed fraud, or financial loss.

WHY THE STAKES ARE HIGH

\$2.4B

REPORTED OLDER-ADULT LOSS

FTC reports for 2024; complaint data undercount total harm.^[9]

4x

GROWTH SINCE 2020

Reported loss among people age 60+ rose from about \$600M.^[9]

7x

HIGH-LOSS REPORTS

Reports over \$100K in imposter scams rose nearly sevenfold.^[11]

**Burden data do not prove a privacy intervention**

Fraud reports establish urgency. Broker, authentication, and intervention research answer different questions and must be interpreted separately.



01

From ordinary data to targeting intelligence

The raw material is often mundane: a deed, a shopping form, a donation, an app permission, a public post, or an old breach. The power comes from linkage, inference, and reuse.



FIVE COMMON SOURCES

A profile is assembled from pieces created for other reasons

The categories overlap, and practices vary by company. The important point is that a person usually does not sit down and create a 'targeting profile.' It is assembled from records and signals generated across daily life.^{[1][2][4][8][20]}

Public records

Property, voter, license, court, marriage, and other government records may reveal age, address, ownership, or relationships.

Commercial activity

Purchases, subscriptions, donations, warranties, loyalty programs, and quote requests can create response and interest signals.

Online activity

Public profiles, posts, advertising identifiers, device signals, and browsing-related data can add context and reachability.

Other brokers

A broker may buy from another broker, merge records, update contact details, or append inferred categories.

Breaches and theft

Stolen credentials and account data enter criminal markets through a different route than lawful commercial brokerage.

People-search sites

Consumer-facing reports can make names, numbers, ages, addresses, properties, and relatives easy to retrieve from one place.

Not all data brokers do the same job

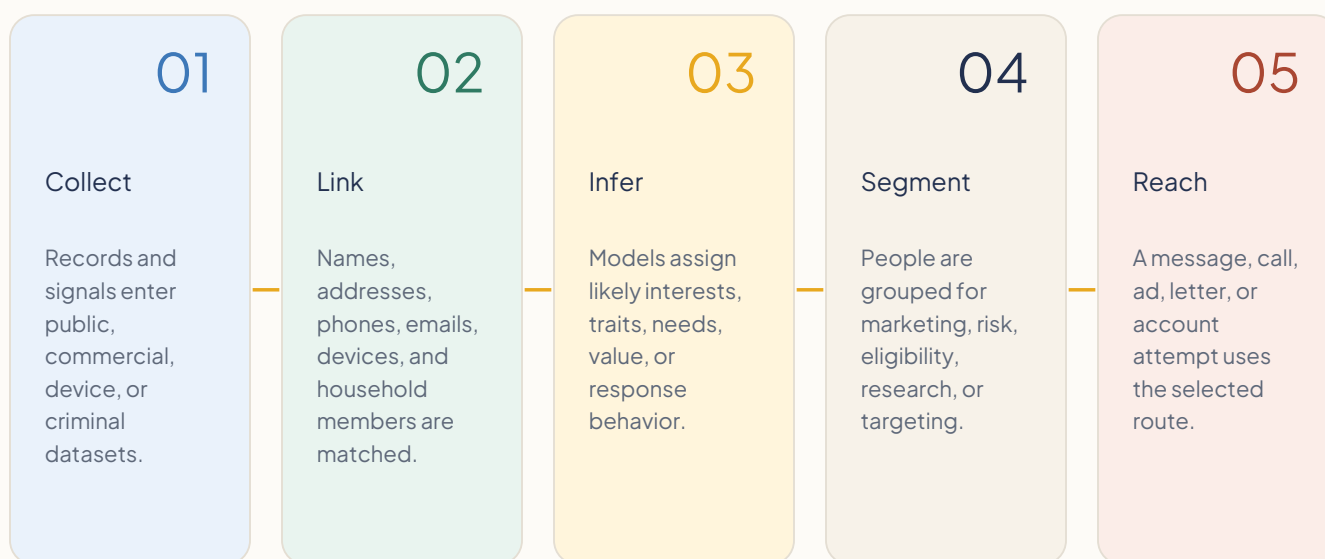
Some support marketing, fraud prevention, identity verification, analytics, or public-record search. Risk depends on the information, the buyer, the purpose, the safeguards, and the ability to correct or delete it.



THE TRANSFORMATION

The risk grows when fragments become a usable story

A phone number is useful for contact. A phone number linked to age, address, family, property, interests, and past responses can support a much more specific approach. The system value comes from combining and updating fragments.



THREE DISTINCTIONS THAT PREVENT BAD CONCLUSIONS

- Available does not mean accurate. Brokered records may be stale, incomplete, or linked to the wrong person.
- Useful does not mean harmful. The same data ecosystem supports identity verification and fraud prevention as well as marketing and abuse.
- Removed from one site does not mean absent everywhere. Public records, relatives' reports, new feeds, and other brokers may still surface it.



The intervention point

A household cannot control every upstream record. It can reduce the easiest public combinations, limit future sharing, and harden the accounts that turn information into access.



A CASE THAT MAKES THE MECHANISM VISIBLE

Epsilon modeled who was most likely to respond – then sold the lists to fraudsters

According to the Justice Department, Epsilon used transactional data and algorithms to predict 'responsive buyers' across a database of 100 million U.S. households. Employees knowingly sold targeted lists to operators sending deceptive sweepstakes and astrology mailings, particularly affecting older and vulnerable people.^{[3][23]}

100M

HOUSEHOLDS IN THE DATABASE

The modeling base described by DOJ at trial.^[3]

218K+

VICTIMS IN ONE SCHEME

A single client used nearly 100 purchased lists.^[3]

\$23.7M

LOSS IN THAT SCHEME

DOJ-described loss associated with the client.^[3]

WHAT THE CASE PROVES

- Targeting data and response modeling can materially facilitate fraud operations.
- Legitimate customer, nonprofit, and charitable relationships can feed data later misused by bad actors.^[23]
- Repeated response can itself become a signal: DOJ said more than 12,000 victims in one scheme were defrauded more than 20 times.^[3]

WHAT THE CASE DOES NOT PROVE

- That every broker or marketing use is fraudulent.
- That a particular opt-out would have prevented the scheme or loss.
- That the same mechanism explains every modern phone, text, social, or account-takeover scam.



Why this case belongs at the center of the paper

It replaces speculation with a documented chain: data, modeling, target selection, contact, repeated response, and fraud harm.

Sources: DOJ sentencing announcement [3]; Epsilon deferred-prosecution agreement [23].



SPECIFIC WITHOUT STEREOTYPING

The relevant difference is the information and stakes – not an assumption about judgment

Older adults report losing money to fraud at a lower rate than younger adults in FTC complaint data, yet they report much higher median losses when loss occurs and are overrepresented in several high-loss scam categories. Age should not be used as a shortcut for incapacity.^[9]

01

Discoverability

Longer public and commercial histories can include property, addresses, licenses, subscriptions, donations, and family links. The mix varies widely by person.

02

Credibility

Accurate names, institutions, purchases, property, and relationships can make an unexpected story feel less random and more familiar.

03

Stakes

Retirement accounts and accumulated assets may make a successful high-loss scheme especially damaging and difficult to recover from.^{[4][9][11]}



A dignity-preserving frame

The task is to redesign exposure and verification around real conditions, not to ask whether an older adult is 'good with technology.' Privacy support should reduce chores while keeping choices and account ownership with the person at the center.

THE FAMILY ROLE

- Ask permission before searching, removing, changing, or monitoring.
- Help with repetitive steps without quietly becoming the owner of accounts.
- Use a trusted second channel when a surprising request involves money, codes, access, or secrecy.

Sources: FTC older-consumer report [9]; GAO retirement-data review [4]; FTC high-loss imposter analysis [11].



02

AI changes the cost of personalization

Generative tools can turn fragments into fluent messages, images, audio, and video. They make production easier. They do not remove the need to reach a person, create pressure, gain access, or move money.



A CHEAPER ASSEMBLY LAYER

AI can make scattered facts sound like one coherent relationship

The FBI describes generative AI being used to produce believable text, fake profiles and identification, synthetic images, cloned audio, and deceptive video. When a sender already has names, relationships, institutions, interests, or recent events, those tools can make personalization faster and more polished.^[10]

WHAT AI CHANGES

Drafting

More fluent messages in many tones and languages.

Synthesis

Faster conversion of fragments into a plausible story.

Impersonation

Cheaper images, profiles, audio, and video.

Scale

More variants and follow-up at lower production cost.

WHAT STILL HAS TO HAPPEN

Reach

A channel still has to connect the sender to the target.

Control

The sender must keep the person inside the attacker's channel.

Action

The person must disclose, install, authenticate, transfer, or pay.

Exit

Independent verification can still break the narrative.

**The defensive implication**

Reducing raw material helps upstream. Independent verification and strong authentication remain necessary downstream because a convincing story can be created from information that cannot be removed.



USEFUL TECHNOLOGY, REAL TRADEOFFS

Aging at home creates more reasons to use data – and more reasons to govern it well

Older adults are already using AI, voice assistants, home security, health tools, and connected services to support independence. The right question is not whether to reject technology. It is what the tool collects, who can access it, what is retained, and whether the benefit is worth the exposure.^{[12][13][14][19]}

55%

USED CONVERSATIONAL AI

U-M poll of adults age 50–97 in February 2025.^[13]

92%

WANT AI DISCLOSURE

Wanted to know when information was AI-generated.^[13]

69%

UNCOMFORTABLE SHARING

AARP: personal health information with a health AI tool.^[19]

QUESTIONS TO ASK BEFORE CONNECTING A TOOL

1

Data

What is collected: voice, video, location, health, activity, contacts, or home routines?

2

Access

Who can see it: the person, family, provider, platform, contractors, advertisers, or researchers?

3

Control

Can the person turn features off, delete history, export records, or revoke family access?

Privacy is part of adoption

AARP's 2026 technology survey identified privacy as the top overall barrier to adoption, while NIST found that understanding and protective action differ by smart-home device category.^{[12][14]}



03

What exposure reduction can – and cannot – do

Deletion, minimization, contact-route separation, and account security act at different points. The strongest plan layers them instead of treating one product or setting as the solution.



REMOVAL IS SPECIFIC, NOT ABSOLUTE

An opt-out removes a listing from a route – not the underlying life record

The FTC explains that people-search sites generally offer free opt-outs. A successful request can stop the site from selling its current listing, but information may remain in public records, appear inside a relative's report, or return when new data arrives.^[1]

WHAT REMOVAL CAN DO

Remove a current profile or matching record from a participating site.

Reduce the easiest public combination of contact, age, address, property, and relatives.

Create a documented request and a reason to recheck later.

Automate repeated requests and monitoring when a service covers the relevant brokers.

WHAT IT CANNOT ESTABLISH

That public records or every downstream copy were deleted.

That a phone number, email address, or identity detail was absent from breaches.

That future records will never recreate a profile.

That removal caused fewer scam attempts, completed frauds, or losses.



The evidence gap

A 2025 preprint tested compliance across 543 registered California data brokers and identified request and verification problems. It helps explain implementation friction; it does not measure fraud outcomes and has not completed peer review.^[17]



CALIFORNIA'S ONE-REQUEST MODEL

DROP changes the mechanics of deletion – beginning August 1, 2026

California residents can now submit one request through the Delete Request and Opt-out Platform to more than 600 registered data brokers. Beginning August 1, brokers must process requests on a recurring cycle and report status. The system does not apply to every company or every record.^{[5][6]}

JAN 2026

Consumer requests open

Eligible California residents can submit a request and choose identifiers.

AUG 1

Broker processing begins

Registered brokers begin matching, deleting, opting out, and reporting status.

EVERY 45 DAYS

The cycle repeats

Brokers access DROP regularly and maintain requests for future matching.

WHAT A CAREFUL EXPLANATION INCLUDES

- **Eligibility:** DROP is for California residents; other states and companies have different rights and processes.
- **Matching:** the identifiers a person provides affect whether a broker can find the record.
- **Scope:** exemptions apply, and a first-party company relationship is different from covered third-party brokerage.
- **Time:** status and deletion are not immediate; updated information may take longer to match and process.



Why this is a national white-paper topic

DROP is a concrete 2026 example of a broader shift from hundreds of individual opt-outs toward persistent, centralized deletion instructions.



REDUCE FUTURE COLLECTION

The least exposed record is often the one never entered

Removal addresses information already held. Data minimization addresses what is supplied next. The goal is not withdrawal from digital life; it is to stop using high-value contact and identity details where they are unnecessary.

1

Separate contact routes

Reserve one email address and phone route for family and important accounts; use a different route for shopping, newsletters, quotes, and public forms.

2

Question the form

Before entering contact or identity data, ask whether the service needs it, who operates the site, and whether a less revealing route is available.

3

Tighten public relationships

Review who can see relatives, travel, schools, employers, birthdays, pets, and other details that can make an approach feel familiar.

4

Review device permissions

Remove unused access to location, contacts, microphone, photos, health data, and advertising identifiers where the function does not need it.

5

Avoid lead-generation traps

Coupon, warranty, insurance-quote, sweepstakes, and similar forms may pass information to multiple marketers or callers.^[20]



A calm default

Use the minimum information needed for the transaction, and keep the primary family and account routes out of low-trust forms.

Source: FTC guidance on information-sharing and unwanted telemarketing [20].



A DIFFERENT LAYER OF DEFENSE

Public information and account access are related – but not the same problem

Removing a people-search listing does not invalidate a stolen password. Strong authentication does not remove a home address. Households need both exposure reduction and access control.

01

Primary email first

Protect the inbox used to reset other accounts. Use a unique password, strong recovery, and multifactor authentication.

02

Use a password manager

Reduce memory burden and password reuse. Save the manager's recovery process somewhere secure and understandable.

03

Prefer stronger MFA

An authenticator app or security key generally provides more protection than a code delivered by SMS, where supported.

04

Consider passkeys

Passkeys can remove password memory burden and provide phishing resistance, but device transfer and recovery need a plan.^{[16][18]}

05

Secure the mobile carrier

Add an account PIN or port-out protection because control of the phone number can affect recovery and texted codes.

06

Save official routes

Use the official app, statement, or bookmarked site rather than a number or link supplied by an unexpected interaction.



Why passkeys matter

NIST treats cryptographic authentication as phishing-resistant because a secret is not manually entered into an impostor site. In 2025 workshops, older adults liked the reduced memory burden but wanted support for setup, transfer, device loss, and shared-device concerns.^{[16][18]}



SEE / SHRINK / STEADY

A privacy plan should end with fewer chores, not a second job

The framework prioritizes the information most useful for reach and credibility, then adds account controls and a light maintenance rhythm. It can be used by an older adult alone or with a trusted person.

01

See

Find the public combinations

Search a name, phone, email, and address safely. Record the profiles that combine contact information with age, property, or relatives.

DO NOW

Choose the one listing that reveals the most useful bundle.

02

Shrink

Remove and stop feeding the trail

Complete high-priority opt-outs, tighten public family details, separate contact routes, and remove unnecessary app permissions.

DO NOW

Finish one real removal or save its exact next action.

03

Steady

Secure and recheck

Harden primary email and financial accounts, save official routes, document recovery, and schedule a light recheck.

DO NOW

Set a 30-day follow-up and quarterly review.



The stopping rule

Do the highest-value work first. A household does not need perfect invisibility; it needs less easy exposure, stronger access controls, and a reliable way to verify surprises.



DESIGN FOR CONSENT AND FOLLOW-THROUGH

Privacy support works better when responsibility is shared clearly

The person at the center should know what is being searched, removed, shared, and monitored. Families, institutions, and technology providers can reduce repetitive work without converting support into surveillance.

01

Older adults

Choose the public details, accounts, and devices that matter most. Keep ownership and recovery routes under your control.

02

Trusted people

Ask permission, help with repetitive steps, save confirmations, and verify surprising requests through an independent route.

03

Institutions

Minimize collection, restrict reuse, make privacy choices understandable, and test whether deletion and suppression actually persist.

04

Product teams

Separate exposure found, records removed, unwanted contact, account compromise, and fraud loss. Do not combine them into one protection claim.

MEASURES WORTH PUBLISHING

- Coverage: which brokers, record types, and identifiers were actually checked?
- Completion: which requests were submitted, matched, deleted, opted out, rejected, or unresolved?



A product claim should name the outcome

'Removed from 60 broker sites' is a removal result. It is not proof of fewer scams or lower loss unless those outcomes were separately measured.



A PRACTICAL COMPANION

The course turns the evidence into one household privacy plan

The forthcoming Personal Data & Privacy Playbook follows the same See / Shrink / Steady structure. It helps an older adult or trusted person complete one removal, strengthen one important account, and save a lightweight maintenance plan.

Chapters 1-3**See the trail**

Run a safe exposure check and identify the combinations that matter most.

Chapters 4-6**Shrink exposure**

Remove a high-priority listing, protect family details, and separate contact routes.

Chapters 7-8**Secure the next step**

Strengthen a critical account and stop unnecessary new collection.

Chapters 9-10**Steady the plan**

Agree on consent, support, and a review schedule without taking over.



Start manually – or use a newer privacy workflow

KinKeeper's free opt-out guides support do-it-yourself removal. Families who do not want to repeat every request by hand can also consider next-generation privacy tools that combine exposure scanning with recurring automated removal, including KinKeeper Privacy.

Availability as of July 15, 2026: Data Removal is rolling out; the public Exposure Scan is pre-launch.^{[21][22]}

kinkeeper.com/opt-out-guides/ | kinkeeper.com/features/privacy/



METHODOLOGY

How this evidence review was assembled

1

Evidence window

Research and official guidance were reviewed through July 15, 2026, with priority to current regulator, law-enforcement, policy, and peer-reviewed sources.

2

Source hierarchy

Primary government sources and original research were preferred. A 2025 preprint was retained only for emerging compliance evidence and is labeled as such.

3

Scope

The review addresses data exposure, targeting, unwanted contact, account security, and reported fraud. It is not a prevalence study or product-effectiveness trial.

4

Synthesis

This is a narrative evidence review. It does not estimate a causal effect for broker removal, automated removal, or any KinKeeper product.

LIMITATIONS

- The data-broker ecosystem is heterogeneous and changes quickly; a practice documented for one company cannot be generalized to every broker.
- Fraud complaint systems undercount harm and are affected by awareness, reporting access, classification, and missing age information.
- Direct evidence of broker data facilitating fraud comes from enforcement cases and may overrepresent the worst conduct.
- Removal studies focus mainly on compliance and process, not randomized or quasi-experimental fraud outcomes.
- Older-adult technology and privacy studies use different populations, countries, methods, and definitions; small qualitative studies inform themes, not rates.



Next scheduled review

October 15, 2026, or earlier if DROP implementation, federal data-broker policy, major enforcement, outcome research, or KinKeeper Privacy availability materially changes.



REFERENCES

Sources 1 of 3

[1] Federal Trade Commission. *What To Know About People Search Sites That Sell Your Information*. July 2022.

<https://consumer.ftc.gov/articles/what-know-about-people-search-sites-sell-your-information>. Accessed July 15, 2026. Primary consumer guidance on data sources, profile contents, opt-outs, verification, reappearance, and the limits of removing current listings.

[2] Federal Trade Commission. *Data Brokers: A Call for Transparency and Accountability*. May 2014.

<https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014>. Accessed July 15, 2026. Foundational regulator study of nine data brokers, their data sources, products, inferred segments, benefits, risks, and transparency gaps.

[3] U.S. Department of Justice. *Epsilon Senior Executive and Sales Manager Both Sentenced for Selling Data on Millions of U.S. Consumers to Fraudsters*. September 30, 2024; updated February 6, 2025.

<https://www.justice.gov/archives/opa/pr/epsilon-senior-executive-and-sales-manager-both-sentenced-selling-data-millions-us-consumers>. Accessed July 15, 2026. Direct enforcement evidence that modeled consumer lists were knowingly sold to fraud schemes targeting older and vulnerable people.

[4] U.S. Government Accountability Office. *Retirement Plans: Department of Labor Guidance Could Mitigate Privacy Risks for Participants*. March 2026.

<https://files.gao.gov/reports/GAO-26-107271/index.html>. Accessed July 15, 2026. Current federal review of retirement-plan data use and sharing, privacy-practice gaps, data-broker risks, and oversight limitations.

[5] California Privacy Protection Agency. *Delete Request and Opt-out Platform (DROP)*. Current July 2026 guidance. <https://privacy.ca.gov/drop/>.

Accessed July 15, 2026. Official consumer guidance for eligibility, request mechanics, identifiers, timing, scope, and limitations of California's DROP.

[6] California Privacy Protection Agency. *Processing DROP Requests*. Current July 2026 guidance.

<https://privacy.ca.gov/drop-for-data-brokers/process-drop-requests/>. Accessed July 15, 2026. Official broker-side requirements beginning August 1, 2026, including 45-day cycles, matching, deletion, service-provider directions, and ongoing suppression.

[7] U.S. Department of Justice, National Security Division. *Data Security Program*. Effective April 8, 2025; current program page.

<https://www.justice.gov/nsd/data-security>. Accessed July 15, 2026. Primary source on restrictions covering access to bulk sensitive U.S. personal data and the recognized risks of commercial data access.

[8] Federal Trade Commission. *FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data*. December 3, 2024.

<https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data>. Accessed July 15, 2026. Recent enforcement concerning collection and sale of precise location information, home identification, consent, and deletion.



REFERENCES

Sources 2 of 3

[9] Federal Trade Commission. *Protecting Older Consumers 2024–2025*. December 2025.

https://www.ftc.gov/system/files/ftc_gov/pdf/P144400-OlderAdultsReportDec2025.pdf. Accessed July 15, 2026. Primary source for reported older-adult fraud losses, high-loss patterns, contact methods, and complaint-data limitations.

[10] Federal Bureau of Investigation, Internet Crime Complaint Center. *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud*.

December 3, 2024. <https://www.ic3.gov/PSA/2024/PSA241203>. Accessed July 15, 2026. Primary source for AI-enabled text, image, audio, and video fraud mechanisms.

[11] Federal Trade Commission. *False Alarm, Real Scam: How Scammers Are Stealing Older Adults' Life Savings*. August 7, 2025. <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/08/false-alarm-real-scam-how-scammers-are-stealing-older-adults-life-savings>. Accessed July 15, 2026. Primary source for high-loss imposter patterns, starting contact channels, payment methods, and population-normalized comparisons.

[12] AARP Research. *2026 Tech Trends and Adults 50–Plus*. December 2025.

<https://www.aarp.org/pri/topics/technology/internet-media-devices/2026-technology-trends-older-adults/>. Accessed July 15, 2026. National survey context on technology use, spending, age-inclusive design, and privacy, trust, and security concerns among adults age 50–plus.

[13] University of Michigan National Poll on Healthy Aging. *How Older Adults Use and Think About AI*. July 2025.

<https://ihpi.umich.edu/national-poll-healthy-aging/national-findings/how-older-adults-use-and-think-about-ai>. Accessed July 15, 2026. National poll of adults age 50–97 on AI use, aging-in-place benefits, trust, disclosure, and desire for risk education.

[14] National Institute of Standards and Technology. *Survey on Smart Home Users' Security and Privacy Perceptions and Actions: A Device Category Perspective*. December 19, 2025.

<https://www.nist.gov/publications/survey-smart-home-users-security-and-privacy-perceptions-and-actions-device-category>. Accessed July 15, 2026. Survey of 401 U.S. smart-home users showing device-specific differences in privacy and security understanding and action.

[15] Akar C, Kocak O, Solmaz U, and Batur Basar T. *Exploring Older Adults' Perceptions of Online Security and Privacy: A Phenomenological Study*.

September 20, 2025. <https://pubmed.ncbi.nlm.nih.gov/40974221/>. Accessed July 15, 2026. Small qualitative study of 14 participants in Turkey; useful for themes of concern, distrust, informal protective strategies, and education needs, not prevalence.

[16] Willis–Arnold B, Vickers P, and Nicholson J. *Are Passkeys the Key? Older Adults' Perceptions of Passwordless Authentication*. September 10, 2025.

<https://researchportal.northumbria.ac.uk/en/publications/are-passkeys-the-key-older-adults-perceptions-of-passwordless-aut/>. Accessed July 15, 2026. Peer-reviewed qualitative workshops with 23 community-dwelling older adults on passkey benefits, device and transfer concerns, and assisted adoption.



REFERENCES

Sources 3 of 3

[17] Khandelwal S, Pavur J, and Wang A. *Consumer Beware! Exploring Data Brokers' CCPA Compliance*. June 27, 2025. <https://arxiv.org/abs/2506.21914>. Accessed July 15, 2026. Emerging preprint reporting a large-scale study of 543 registered brokers; used for compliance and verification friction, with preprint status disclosed.

[18] National Institute of Standards and Technology. *NIST SP 800-63B-4: Digital Identity Guidelines - Authentication and Authenticator Management*. August 1, 2025. <https://www.nist.gov/publications/nist-sp-800-63b-4digital-identity-guidelines-authentication-and-authenticator>. Accessed July 15, 2026. Current technical guidance on passwords, authenticators, phishing resistance, recovery, and cryptographic authentication.

[19] AARP Research. *Adults Age 50-Plus and AI-Powered Health Tools Survey*. June 11, 2026. <https://www.aarp.org/pri/topics/technology/internet-media-devices/artificial-intelligence-health-tools/>. Accessed July 15, 2026. Probability-based national survey on AI health-question use, privacy concerns, data-sharing expectations, and trust among adults age 50-plus.

[20] Federal Trade Commission. *When Sharing Your Info Online Leads to Unwanted and Unlawful Telemarketing Calls*. September 2025. <https://consumer.ftc.gov/consumer-alerts/2025/09/when-sharing-your-info-online-leads-unwanted-and-unlawful-telemarketing-calls>. Accessed July 15, 2026. Recent enforcement-linked guidance explaining how online quote, coupon, sweepstakes, and warranty forms may lead to resale and unwanted contact.

[21] KinKeeper. *Data Broker Opt-Out Guides*. Current July 2026 resource collection. <https://www.kinkeeper.com/opt-out-guides/>. Accessed July 15, 2026. Companion manual-removal guides. Product and course context only; not used as external evidence.

[22] KinKeeper. *Privacy*. Current July 2026 product page. <https://www.kinkeeper.com/features/privacy/>. Accessed July 15, 2026. Product-context source. Data Removal is rolling out and Exposure Scan is pre-launch as of the evidence cutoff. Not used as proof of external outcomes.

[23] U.S. Department of Justice. *Marketing Company Agrees to Pay \$150 Million for Facilitating Elder Fraud Schemes*. January 27, 2021. <https://www.justice.gov/archives/opa/pr/marketing-company-agrees-pay-150-million-facilitating-elder-fraud-schemes>. Accessed July 15, 2026. Epsilon deferred-prosecution agreement, admitted sale of data associated with more than 30 million consumers to fraudulent schemes, victim compensation, and compliance measures.



KinKeeper helps families coordinate daily Wellbeing check-ins and protection across Privacy, Money, and Identity. The Kin Circle receives outcomes, summaries, and alerts while the person at the center keeps their independence.

Two 15 Foundry, LLC dba KinKeeper | kinkeeper.com | Research edition 1.0