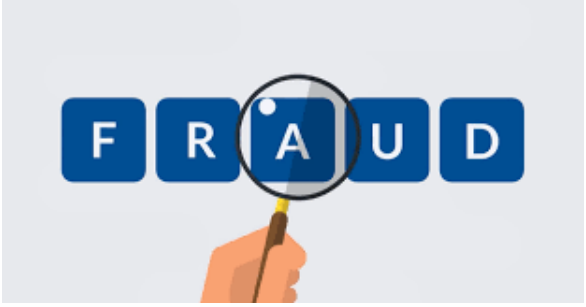
Financial Fraud Prevention and Detection Tips



Presented by:

Iowa Bankers Association

IOWA BANKERS ASSOCIATION

1

2024 Financial Fraud Statistics

- Federal Trade Commission Report
  - 2.6 million consumers reporting
  - $12.5 billion lost due to fraud (increase of 25%)
- More people losing money
  - Email and phone; Iowans reported losing nearly $47.8 million (FBI reports $72 million in losses)
- Increasing sophisticated fraud attempts
  - Use of Generative AI
  - Investment scams highest reported losses ($5.7 billion)
  - Imposter scams losses ($2.95 billion)
- Payment Method: bank transfers and cryptocurrency

https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024?utm_source=govdelivery

2

Scams

Scam	Definition
Grandparent	Story that compels grandparents to send money to help (Don't tell mom!)
Romance	Fake romantic relationship to emotionally manipulate victim
Investment	Lure victim with fake/misleading investment opportunity
Fake Prize	Informs victim they won a prize; owe taxes to collect
Imposter	Impersonate gov't, business, other officials/agencies
Elder Financial Exploitation	Targets older adults. Involves deception, coercion, exploitation
Fake Distress	Pretends to be a relative or friend in urgent need of money
Identity Theft	Uses another person's personal identifying info to commit financial crimes
Money Laundering	Process of disguising illegally obtained funds to make them appear legitimate

3

Scams

Scam	Definition
Ecommerce	Use of stolen payment information to make purchases online/set up fake online stores
Account Takeover	Unauthorized access to and control over person's financial account
Phishing - Social Engineering	Impersonates legitimate entities via email, phone call, fake website to gain revealing sensitive account credentials
Malware	Malicious software secretly installed on device to steal financial data, spy on activities, gain control over accounts
Social Media	Conducted through social platforms (selling stolen/fake goods, fake giveaways, impersonation accounts, phishing links)
Payment App	Involves digital payment apps tricking user into sending funds

4

Scam Methods

Scam	Definition
Wire Transfer	Tricks into sending funds via wire (trusted contact, romance)
Gift Card	Tricked into buying/selling gift cards (imposter)
Credit Card	Unauthorized use of a person's credit card info
Debit Card	Illicit use of debit card/account number to withdraw money or conduct transaction
Loan	Fraudulently obtaining a loan through misrepresentation of personal, business or financial information; using funds in fraudulent manner; using stolen identity to secure loan
ATM	Illegitimate access to bank account via ATM (can include jackpotting – introduced malware causing it to dispense funds to scammer)

5

Scams

Scam	Definition
Skimming	Use of hidden device placed on ATM or card reader to steal card info during legitimate transaction
Card trapping	Device inserted into ATM to capture card's info; used to clone additional cards.
Forgery	False making of document
Counterfeit	Production or use of fake financial instruments (currency, checks, cards)
Check Kiting	Exploiting float time by writing checks from one account with insufficient funds to another (creates illusion of funds)
Alteration	Illegally changing details on legitimate financial document (check, invoice) to increase payment or redirect funds

6

Fraud Types

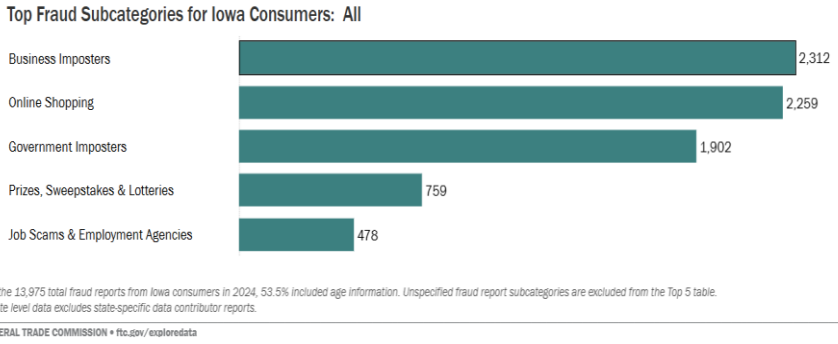
- Checks – payment method most vulnerable to fraud
  - 10% increase in USPS interference
- Electronic transactions - Due to Business Email Compromise, ACH credit fraud surpasses wires

Top Payment Methods Impacted by Business Email Compromise, 2019-2023
(Percent of Organizations)

	2023	2022	2021	2020	2019
ACH credits	47%	34%	41%	34%	37%
Wire transfer	39%	45%	41%	43%	42%
ACH debits	20%	26%	14%	16%	21%
Checks	18%	16%	19%	14%	19%

Fraud Types

- Top Fraud Subcategories for Iowa



Iowa Consumers

Iowa Consumers
Year: 2024

State Name: Iowa | Year: 2024 | Quarter: (All)

Fraud Reports and Losses

Consumer Age	# of Reports	% Reporting $ Loss	Total $ Loss	Median $ Loss
19 and Under	203	46.3%	$50,887	$1[illegible]
20 - 29	840	37.9%	$1,587,625	$396
30 - 39	1,124	36.3%	$2,5[illegible]35	$300
40 - 49	1,198	34.8%	$3,632,473	$370
50 - 59	1,062	32.5%	$4,166,852	$500
60 - 69	1,523	26.1%	$7,432,735	$70[illegible]
70 - 79	1,133	23.5%	$3,329,039	$1,044
80 and Over	389	14.9%	$662,396	$2,000

Highest # of reports – older adults

Highest % of losses – younger adults

9

Impersonation Scams

- Government Impersonation Scams
  - Multi agency efforts to raise awareness
    - FTC, DOJ, FBI, USPIS, IRS, SSA, CBP, DOL, SEC, DHS, VA, and Federal Reserve
  - Losses from gov't impersonation scams topped $618M in 2023
  - Targets consumers for payments in cash (provided in-person or via mail)
    - Cash payment losses nearly doubled from 2022 to 2023
      - Q1 2024: $20 million (est. $80 million+ for year)
      - 2023 - $76 million
      - 2022 - $40 million
  - Report to FTC at ReportFraud.ftc.gov

10

Deepfake Media

- FIN-2024-Alert004 issued Nov. 13, 2024
- Help FIs identify fraud schemes associated with the use of deepfake media created with generative artificial intelligence tools (GenAI)
- Criminals have used GenAI to create falsified documents, photographs, and videos to circumvent bank CIP identification and verification programs
  - E.g., create or alter ID documents
  - E.g., create fake video images

Deepfake Media

- Identity-related exploitation is major cyber crime and fraud concern for banks
- Methods to Detect Gen AI and Synthetic Content
  - Re-review account opening documents
  - Investigate suspected deepfake images
    - Conduct reverse image searches and use other open-source research revealing identity photo matches an image on online gallery
- Train Staff on Red Flags

Deepfake Media

- Deepfake Red Flags
  - Customer's photo is inconsistent with other identifying information or appears to have been altered
  - Customer uses 3rd party webcam plugin during live verification check
  - Customer attempts to change communication methods during live verification check due to "technology glitches"
  - Customer declines use of multi-factor authentication to verify their identity

13

Deepfake Media

- Deepfake Red Flags
  - Reverse image look up of identity photo matches an image in online gallery of AI-produced faces
  - Gen AI-detection software flags the potential use of Gen AI text in a customer's profile
  - A customer's geographic or device data is inconsistent with the customer's identity documents
  - A newly opened account or an account with little prior transaction history has:
    - A pattern of rapid transactions
    - High payment volumes to potentially risky payees, such as gambling websites or digital asset exchanges; or
    - High volumes of chargebacks or rejected payment

14

Deep Fake Media

https://www.aba.com/-/media/documents/infographics/2025-aba-foundation-deep-fake-infographic-web.pdf?rev=2299e1f127cc4071893d61234f1844c1

Gen AI and FBI

- Alert issued Dec. 3, 2024
- Warning to public – criminals' exploitation of Gen AI to commit fraud using technology to:
  - Create fictitious social media providers
  - Create messages to trick victims into sending money
  - Create realistic images and documents used in identity fraud and impersonation schemes
  - Voice cloning to obtain access to bank accounts or to trick victims that a relative is in crisis

Gen AI and FBI

- Tips for Customers:
  - Create a secret word or phrase with family
  - Look for subtle imperfections in images/videos
  - Listen closely to tone and word choice
  - Limit online content of your image or voice, make social media accounts private, and limit followers
  - Verify identity of person calling by hanging up and calling known number directly
  - Never share sensitive information with new people met online or over phone
  - Don't send money, gift cards, cryptocurrency to new people

Counterfeit U.S. Passport Cards

- FIN-2024-NTC1 Issued April 15, 2024
- U.S. Passport cards – REAL ID compliant for identity, domestic air travel, and citizenship
- Increase in counterfeit U.S. passport cards to gain access to victim accounts
- Fraud rings falsely making, selling and using counterfeit cards
- Impersonates victim by using counterfeit U.S. passport card that contains victim's info

Counterfeit U.S. Passport Cards

- From 2018 to 2023 resulted in $10M in losses with additional $8M in attempts (over 4,000 victims)
- Successful because U.S. passport cards are less familiar form of government-issued IDs
- Use branches not frequently used by victim
- Fraudster or Money Mule may use to:
  - Gain information (balance, w/d limits) to withdraw cash
  - Cash stolen/forged checks
  - Open new accounts

19

Legitimate U.S. Passport Card

1 – Holographic security feature

2 – Patch of color shifting ink

3 – Textured, clear artwork of Great Seal of US

4 – Card bearers date of birth (deep black with texture)

5 – large portrait in grayscale containing fine lines

6 – small portrait containing text with info specific to card owner

7 – colorful background artwork containing tiny text

8 – Invisible printing only detected by UV light

20

Counterfeit U.S. Passport Cards

- Behavioral Red Flags
  - May not know date of birth or SSN
  - Appears to be following directions by phone from third-party
  - Customer transacts at branch outside their geographical footprint
- Financial Red Flags
  - Presents U.S. Passport Card for withdrawals, purchase of cashier's checks or initiates wires for large amounts
  - Attempts to negotiate uncharacteristic, sudden or abnormally large volume of checks payable to cash

CVC Kiosks

- FIN-2025-NTC1 – Issued Aug. 4, 2025
- Notice of use of CVC kiosks for scam payments and other illicit activities
  - Fraud schemes
  - Drug trafficking
  - Cybercrime

- CVC kiosks facilitate exchange of cash or cards to cryptocurrency
  - Significant fees for some operators
  - Required to register as MSB
- Scams targets elderly

CVC Kiosks

- Red Flags
  - Multiple payments just below SAR reporting threshold from multiple kiosk locations
  - Limited or no transaction history makes substantial deposit that is rapidly transferred into CVC
  - In-person transaction withdrawing substantial amounts of cash from accounts (MMDA, CDs, IRAs) after being directed to do so by person on phone/internet
  - Using geographically disparate locations to make deposits to same CVC address over short period

Sextortion

- FIN-2025-NTC2 issued Sept. 8, 2025
- Assist in identifying and reporting suspicious activity related to financially motivated sextortion
  - Use fake personas to coerce victims to create and send sexually explicit images/videos
  - Threatens to release to friends/family if payment is not received
  - Many victims over age 18
    - Common target – boys between 14 and 17
    - Has led to alarming number of suicides
  - Provides payment methods and red flags
  - Provides SAR filing instructions

How to Stay Informed - FinCEN Alerts

Title	Date	Description
FIN-2025-NTC1	8/4/2025	Notice on Use of Virtual Currency Kiosks for Scam Payments and Other Illicit Activity
FIN-2024-Alert005	12/18/24	Alert on Fraud Schemes Abusing FinCEN's Name, Insignia, and Authorities for Financial Gain
FIN-2024-Alert004	11/13/24	Alert on Fraud Schemes Involving Deepfake Media Targeting FIs
FIN-2024-Alert003	10/23/24	Alert to FIs to Counter Financing of Hizballah and its Terrorist Activities
FIN-2024-Alert002	7/11/24	Supplemental Advisory on Procurement of Chemicals and Equipment Used for Synthesis of Illicit Fentanyl and Other Synthetic Opioids.

Full List: FinCEN Guidance Related to SAR Filings (IBA Document)

25

Fraud Defense

- Customer Identification Program
  - Identification documents
  - Discrepancies
  - If unfamiliar, don't have to accept
  - KNOW YOUR CIP
- Customer Due Diligence
  - Understand how account will be used
  - Ask pertinent questions
  - Try to identify risky behavior
- Monitor based on risk

26

Fraud Offense

- Suspicious
  - Do not need to determine activity is illegal
  - Doesn't have to be a loss (attempts count!)
  - Don't fit usual pattern of activity for that customer/business
  - Lacks clear economic purpose
- Indicators
  - Unusual transaction size or frequency
  - Geographic anomalies
  - Inconsistent
  - Complex or unusual patterns
  - Anonymous transactions

Investigative Context

- Individually, indicators ***not definitive proof of wrongdoing*** – signals that require further investigation
- Use judgement, experience and knowledge of customers to assess transaction vs. behavior and patterns
  - Review alerts
  - Conduct preliminary assessment
  - Gather information
  - Determine context – look for inconsistencies, transaction patterns, identify connections to others (known criminals, watchlists, etc.)

Decision Time

- Make decision based on analysis
- If suspicious, refer to BSA officer for possible SAR filing
- Consider closing account
- Document each step of investigation
- Update system where appropriate
  - Customer risk profile
  - Alerts

Privacy and Fraud When Can We Share?

Information Sharing

- Privacy Statutes:
  - Gramm-Leach-Bliley (GLBA)
    - Protects consumer's non-public personal information
    - Exceptions apply for sharing with local, state or federal authorities:
      - Responding to civil, criminal or regulatory investigation, subpoena or summons
      - To protect against/prevent fraud or potential fraud, unauthorized transactions, etc.
      - Reporting suspected financial abuse to proper agency or law enforcement

Trusted Contact

- GLBA does NOT permit:
  - Sharing of NPPI with persons NOT authorized on the account without consent
    - E.g., transaction information with family member NOT authorized on the account or appointed as custodian or agent for elder customer
- Trusted Contact
  - Consider obtaining account owner's consent to disclose account info to trusted party if bank suspects fraud
  - Not a legal concept – agreement developed by bank's legal counsel

Trusted Contact Program

- Information that may be included
  - What situations would trigger sharing?
  - What information can be shared?
  - Will this require notice to accountholder?
  - Can it be rescinded?
  - Method to rescind and timeframe?
- Single form may not be appropriate
  - May need to be modified based on customer's request
- Agreement must be documented

Suspicious Activity Reports

- Required to report suspicious activity
- Not required to prove illegal!
- SAR mandatory Reporting Thresholds (aggregate):
  - $5,000 if subject known
  - $25,000 if subject not known
  - $0 if insider abuse
- Voluntary reporting permitted below threshold
- BSA protection if report to appropriate authorities when file SAR

BSA Voluntary Reporting

- BSA encourages reporting suspected elder abuse to appropriate law enforcement or agencies
- Privacy rules do not prohibit it
- Reporting may help stop the abuse/fraud

Elder Financial Exploitation

- Interagency Guidance
  - Released Dec. 4, 2024
  - Provides examples of risk management practices for identifying, preventing and responding to EFE
- Governance and Oversight
  - Consider enhancing or creating risk-based policies, internal controls, employee codes of conduct, ongoing monitoring and complaint processes
    - Caution: Ensure policies do not result in age discrimination under ECOA

Elder Financial Exploitation

- Employee Training
  - Include red flags, provide proactive approaches and detailed actions to take when concerns are identified
- Use Transaction Holds and Disbursement Delays
  - Reg. CC rules for holds
  - State laws that may permit temporary holds
- Use Trusted Contact Program
- File SARs
  - Can voluntarily file
  - Reminded of confidential nature of SARs

37

Elder Financial Exploitation

- Report to:
  - Law enforcement in accordance with GLBA
  - Adult Protective Services as state law allows (Iowa Health & Human Services)
- Refer victims to:
  - DOJ for assistance
    - National Elder Fraud Hotline – 833-372-8311
  - FTC via Internet Crimes Complaint Center (IC3.gov)
  - U.S. Postal Inspection Service
  - SSA or other federal state or local agencies
- Engage in consumer outreach and awareness

38

Iowa State Law

Section	Key Definitions
235B.3(4) Dependent Adult	• "An employee of a financial institution *may* report suspected financial exploitation of a **dependent adult** to the department" • "Dependent adult" - a person **eighteen years of age or older** who is **unable to protect their own interests** or unable to adequately perform or obtain services necessary to meet essential human needs, **as a result of a physical or mental condition** which requires assistance from another.

235F Vulnerable Elder	• Vulnerable elder - **Sixty years of age** or older **and** **unable to protect himself** from elder abuse due to:
	  • Age or mental/physical condition
	  • Personal circumstances which results in increased risk of harm
	• *Financial Exploitation* - Person standing in position of trust using influence, deception, coercion, fraud or extortion, contains control over/uses/diverts benefits, property, resources, belongings or assets

633B.120 POA Abuse	• Effect on POA – allows bank to refuse POA if certain conditions exist

39

EFE Federal Law – 65+

- EGRRCPA
  - Signed into law May 2018
  - Section 303
    - FI may not be liable, including in any civil or administrative proceedings, for disclosure to covered agency
    - Refers to suspected exploitation of a **senior citizen**
    - Only covers bank employees that received proper training

Covered Agency
- State financial regulatory agency (e.g., state securities or law enforcement authority and state insurance regulator)
- Each of the Federal prudential regulators represented by the FFIEC
- SEC
- Law enforcement agency
- State or local agency responsible for administering adult protective service laws

40

EFE Federal Law

- Exploitation under EGRRPRA
  - Fraudulent or otherwise illegal, unauthorized, or improper act or process of an individual, including a caregiver or fiduciary
  - Uses resources of senior citizen for monetary or personal benefit, profit or gain
  - Deprives a senior citizen of rightful access to or use of resources, benefits or assets
  - Applies to **individuals 65 year or older**
    - No requirement they be a dependent adult

EFE Federal Law

- EGRRPRA Training Requirement
  - Employee reporting fraud
  - Employees who come in contact with senior citizens as regular part of professional duties
  - Employee/officer who may review/approve financial documents
- Timing:
  - As soon as practicable
  - No later than one year after employment date

IBA Resources

- **BANK ARSENAL TO DEFEND AGAINST FRAUD WEBINAR SERIES**
  - Part 1: Bank Arsenal to Defend Against Check Fraud (1/23/2024) presentation PDF
  - Part 2: Check Fraud: Breach of Warranty Claims (2/7/2024) presentation PDF
  - Part 3: Check Fraud: Official Checks and Treasury Checks (2/21/2024) presentation PDF
  - Part 4: Debit Card Fraud (3/6/2024) presentation PDF
  - Part 5: Wire Fraud (3/20/24) presentation PDF
  - Part 6: ACH Fraud (4/3/24) presentation PDF
  - Part 7: Money Mules (4/16/24) presentation PDF

43

IBA Resources

- Fraud Resources
  - Videos (Money Cents Campaign)
  - Articles
  - Downloads (presentation templates)
  - State of Iowa – Cybersecurity
  - Organizational
    - AARP Fraud Watch Network
    - NCA Stay Safe Online
  - AND MORE!

Federal Resources

- Federal Reserve Tool Kits for Fraud Mitigation
- CFPB Consumer Tools
- CISA – Shields Up
- FDIC Consumer Resource Center
- FTC Consumer Advice
- OCC Fraud Prevention Resources
- SSA Protect Yourself from Scams

44

Tools & Resources

- More IBA BSA Tools
  - SAR filing instructions to FinCEN
  - Possible Suspicious Activity Form
  - SAR Incident Determination Report
  - Suspicious Activity Log
- FTC Fraud
  - Scams and Your Small Business
  - Shopping and Donating
  - Jobs and Making Money
  - Unwanted Calls, Emails, and Texts
  - Identity Theft and Online Security Scams

Tools & Resources

- ABA tools
  - Fraud Prevention
  - Elder Financial Exploitation
  - Identity Theft Tool Kit
  - ABA Fraud Contact Directory
  - Banks Never Ask That/Practice Safe Checks
- CFPB Tools
  - Common scams
  - Understanding identity theft
  - How to protect yourself and others

Tools & Resources

- Visa – Security & Trust
  - Consumer Training related to:
    - Romance Scams
    - Executive Impersonation Scams
    - Data and AI
    - Holiday scams and shopping tips