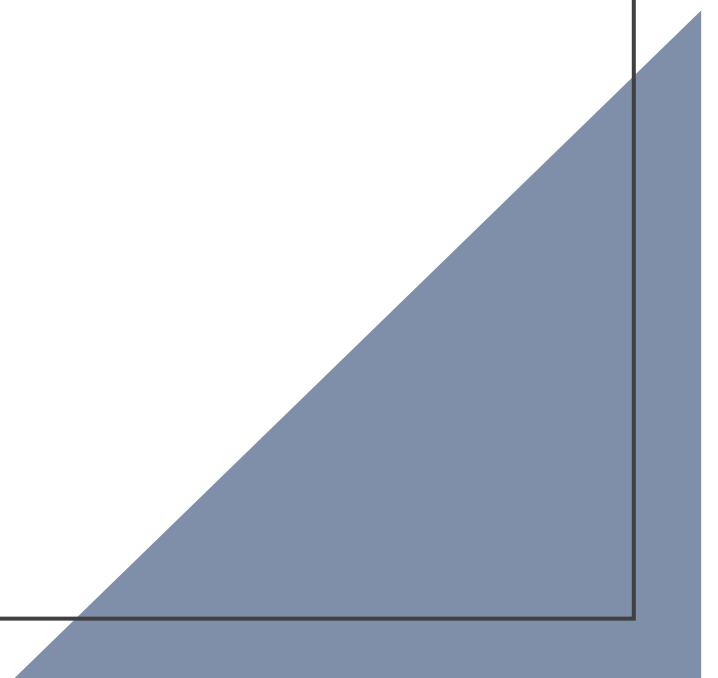


Protecting Yourself from Fraud

By the Hennepin County Attorney's Office



What are we discussing today?

1

Defining “fraud” and
“identity theft”

2

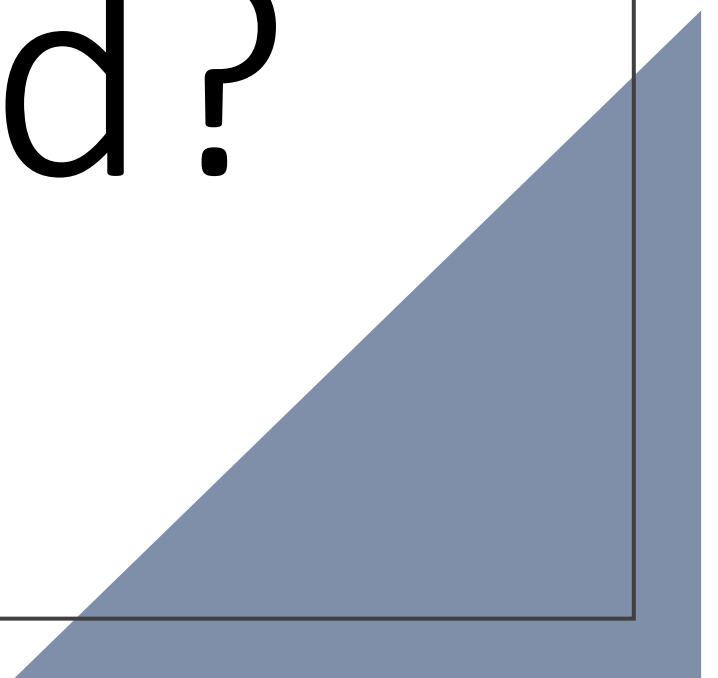
How to spot fraud

3

How to report a
fraud

What is fraud?

When someone lies to you to **take something of value** (money, personal information, or property).



Fraud = Scam

“Fraud” and “scam” mean the same thing. I will be using both words interchangeably.

What is identity theft?

A type of fraud that **targets personal information** instead of money or property.

TYPES OF ABUSE > Financial Exploitation

Exploiters may describe themselves as “family caregivers,” while the truth is that they are dependent on their victims for financial assistance, housing and other support. The risk increases when the exploiter knows where important papers are and has access to personal information (e.g., PIN numbers, Social Security number). Substance abuse and other personal problems may be associated with the behavior.

Financial exploitation happens in many ways. These include when someone who has a legal obligation to manage the money makes unauthorized expenditures of a vulnerable adult’s funds, or fails to use the funds for his/her food, clothing, shelter, health care or supervision. Financial exploitation can also occur when someone uses or disposes of a vulnerable adult’s money or property without any legal authority.

Acquiring possession or control of a vulnerable adult’s funds or property through pressure, deception, or fraud constitutes financial exploitation.

How to Spot Fraud



PRETEND: Fraudsters pretend to be from a credible organization



PROBLEM OR PRIZE: Fraudsters will say you're in trouble or won big



PRESSURE: Fraudsters will push you to act immediately



PAY: Fraudsters will insist that you send money through digital means, gift cards, or checks to avoid meeting in-person

How Do
Fraudsters
Contact You?

Susceptibility and monetary loss by means of contact

MEANS OF CONTACT	SUSCEPTIBILITY	MEDIAN \$ LOSS
Website	73.7%	\$100
Social media (e.g., Facebook)	72.0%	\$90
Email	40.0%	\$239
Phone	17.9%	\$573
Internet messaging (e.g., WhatsApp)	50.7%	\$436
Text message	21.4%	\$630
Online classifieds (e.g., Craigslist)	52.3%	\$238
In person	56.6%	\$700
Postal mail	10.3%	\$150

Frequently Impersonated Organizations

TABLE 7

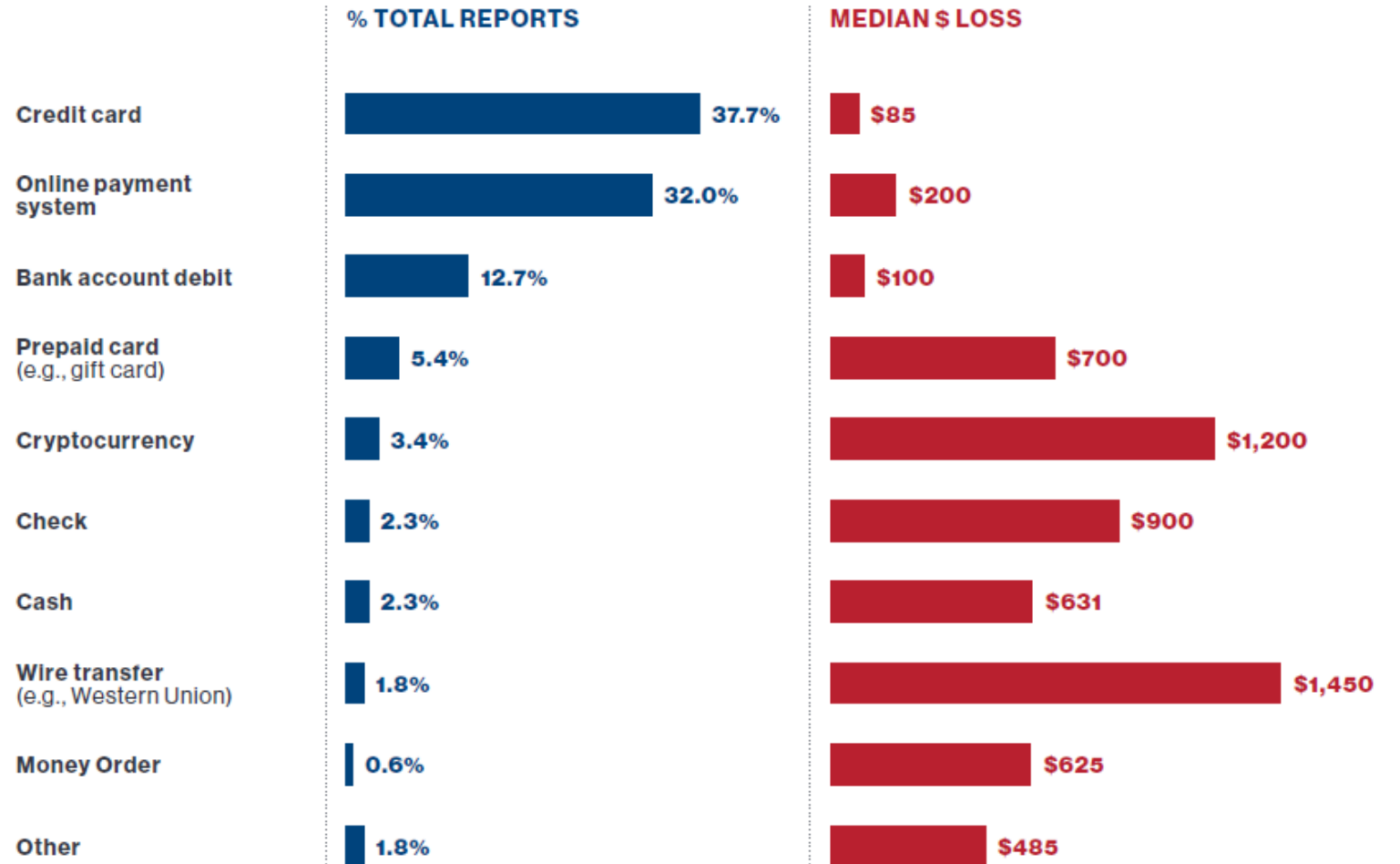
Top 10 organizations/brands used for impersonation

RANK	BUSINESS NAME	SCAMS
1	Amazon	1,460
2	Social Security Administration	697
3	Publishers Clearing House	395
4	PayPal	181
5	Medicare	149
6	Microsoft	137
7	Apple	125
8	Walmart	118
9	Cash Advance/Advance America	95
10	Facebook	90

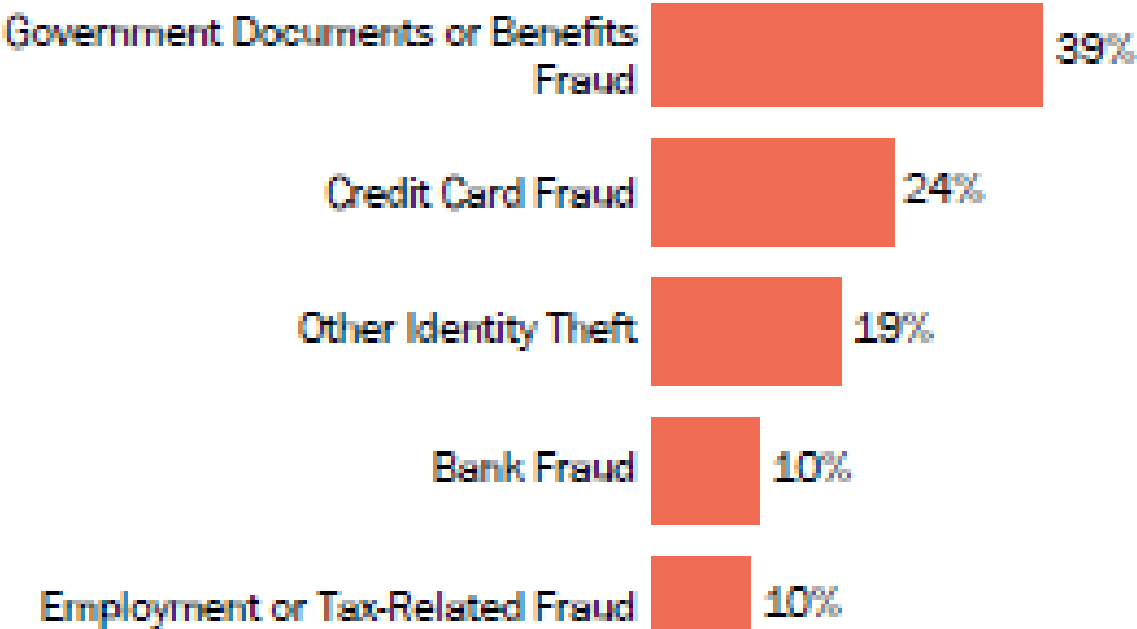
Payment Methods that Scammers Love

FIGURE 12

Percent of total scam reports resulting in monetary loss by payment method



Top Identity Theft Types

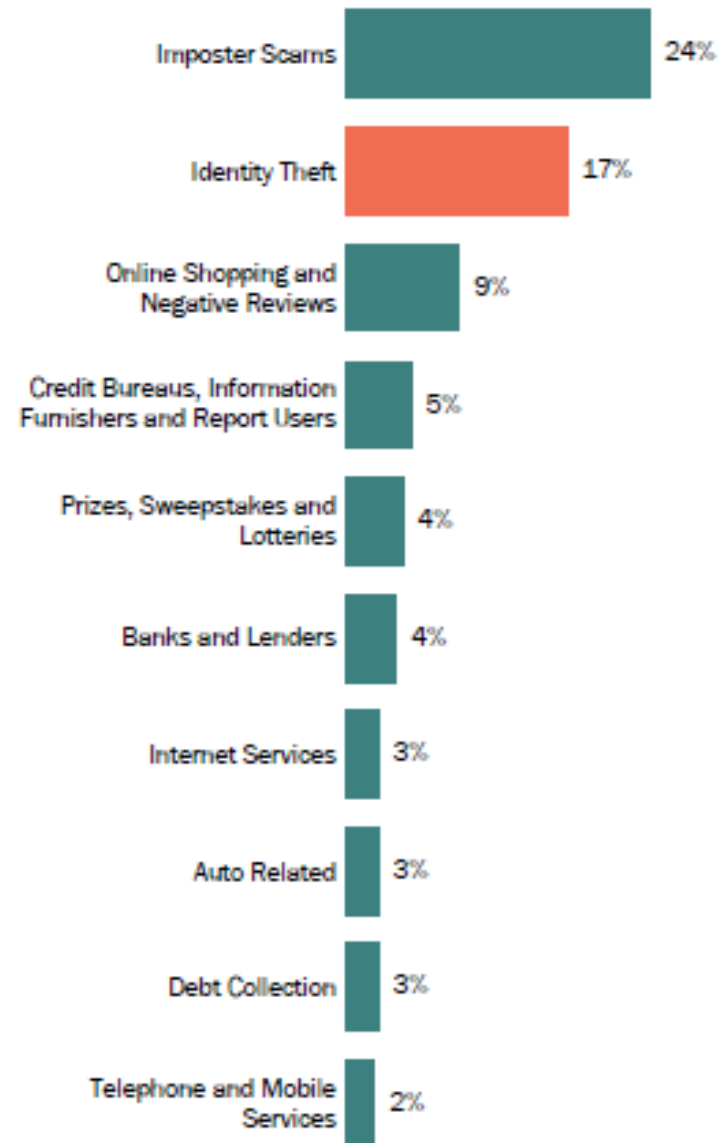


What are Identity Thieves looking for?

Most
common
types of
fraud in MN:

Minnesota

Top Ten Report Categories



Fraud Losses

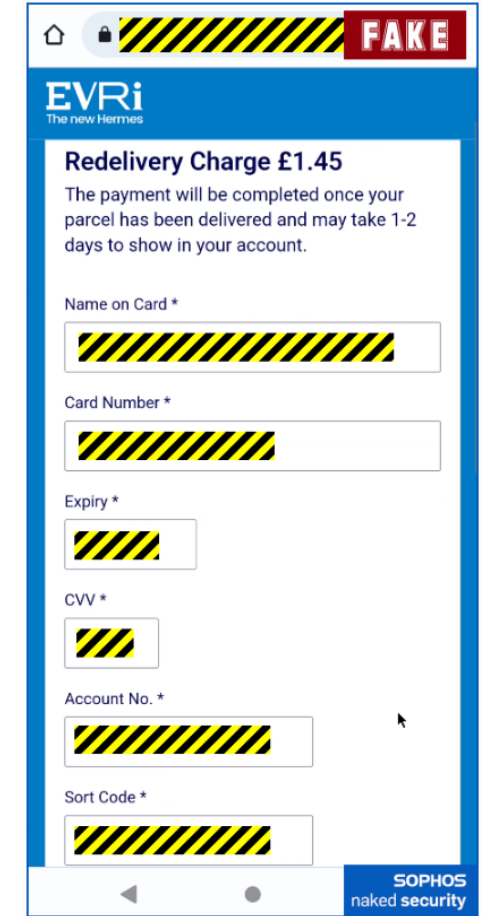
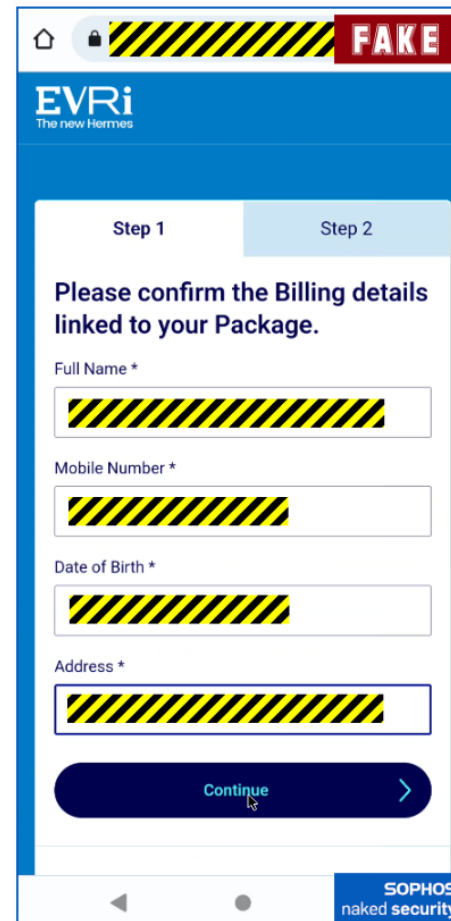
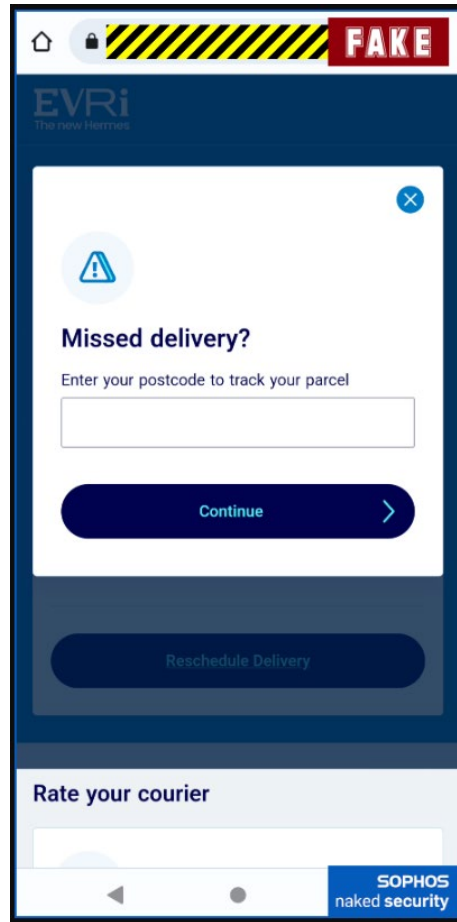
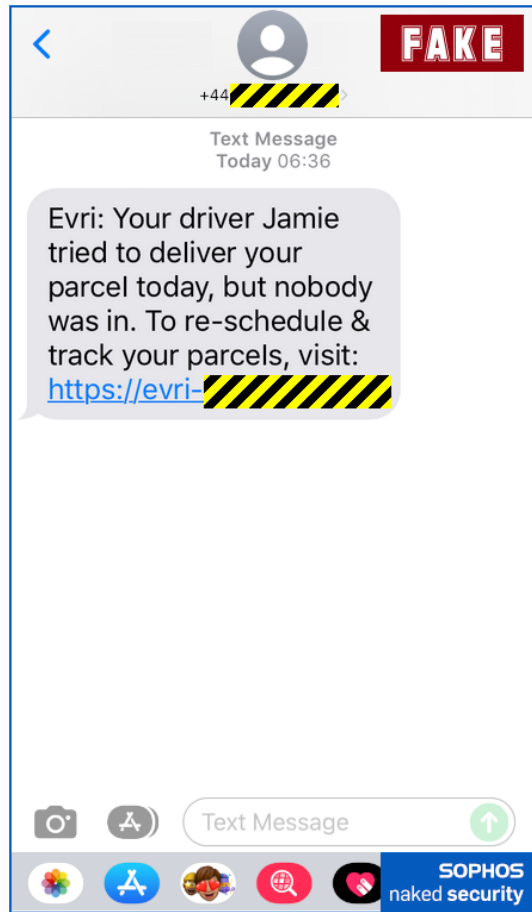
\$60.3M

Total Fraud Losses

\$482

Median Fraud Losses

What can Phishing look like?





PHISHING SCAMS

ROMANCE SCAMS

YOU'VE WON!
SCAMS

BOGUS JOB
SCAMS

SHOPPING SCAMS

MOST COMMON FACEBOOK SCAMS



FAKE CHARITY
SCAMS

FACEBOOK
QUIZ SCAMS

FAKE FRIEND
REQUESTS

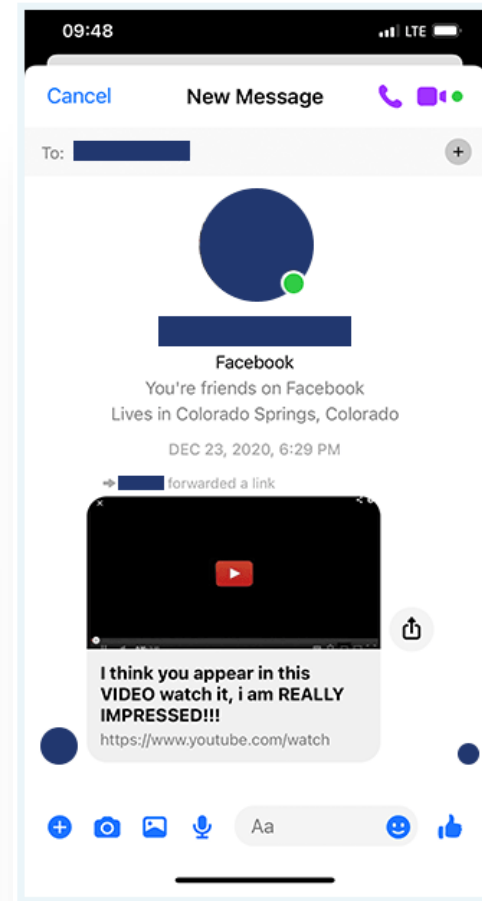
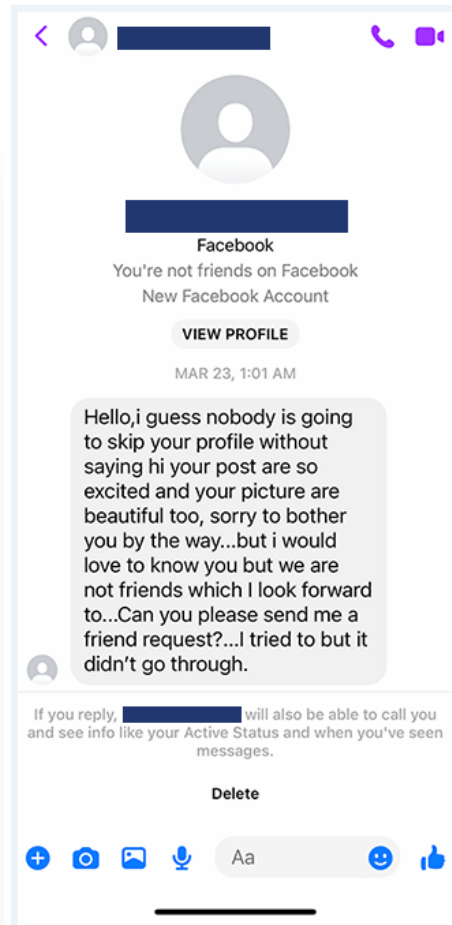
SUSPICIOUS LINKS
ABOUT YOU

FAKE COUPONS
AND DISCOUNTS



What about
Social Media
Scams?

Examples of Facebook Scams



2021 Fraud Statistics

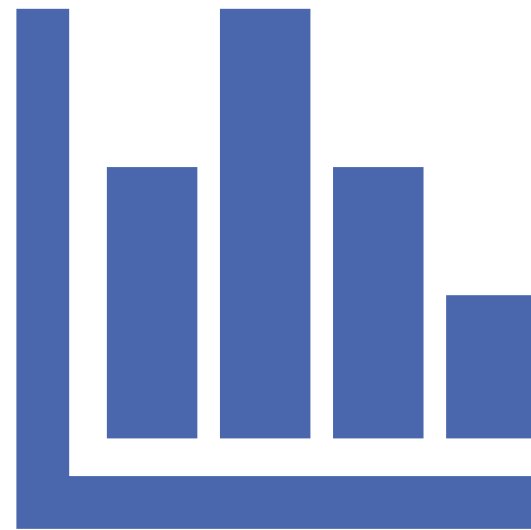


TABLE 1
10 riskiest consumer scams in 2021

RANK		SCAM TYPE	BBB RISK INDEX	EXPOSURE		SUSCEPTIBILITY		MEDIAN \$ LOSS	
2021	2020			2021	2020	2021	2020	2021	2020
1	1	Online purchase	167.4	37.4%	38.3%	74.9%	78.8%	\$101	\$96
2	7	Cryptocurrency	90.6	1.9%	0.7%	66.2%	55.8%	\$1,200	\$1,200
3	2	Employment	63.0	7.8%	7.1%	15.1%	16.6%	\$900	\$967
4	5	Home improvement	45.2	1.4%	0.7%	59.1%	58.7%	\$955	\$1,193
5	10	Investment	29.9	0.8%	0.6%	56.9%	67.2%	\$1,100	\$948
6	3	Fake check/ money order	27.1	2.1%	2.7%	14.8%	16.6%	\$1,475	\$1,679
7	4	Advance fee loan	25.9	1.8%	1.6%	40.6%	47.1%	\$609	\$745
8	13	Government grant	24.8	2.2%	2.0%	19.5%	15.9%	\$1,000	\$800

Riskiest Scams by Age

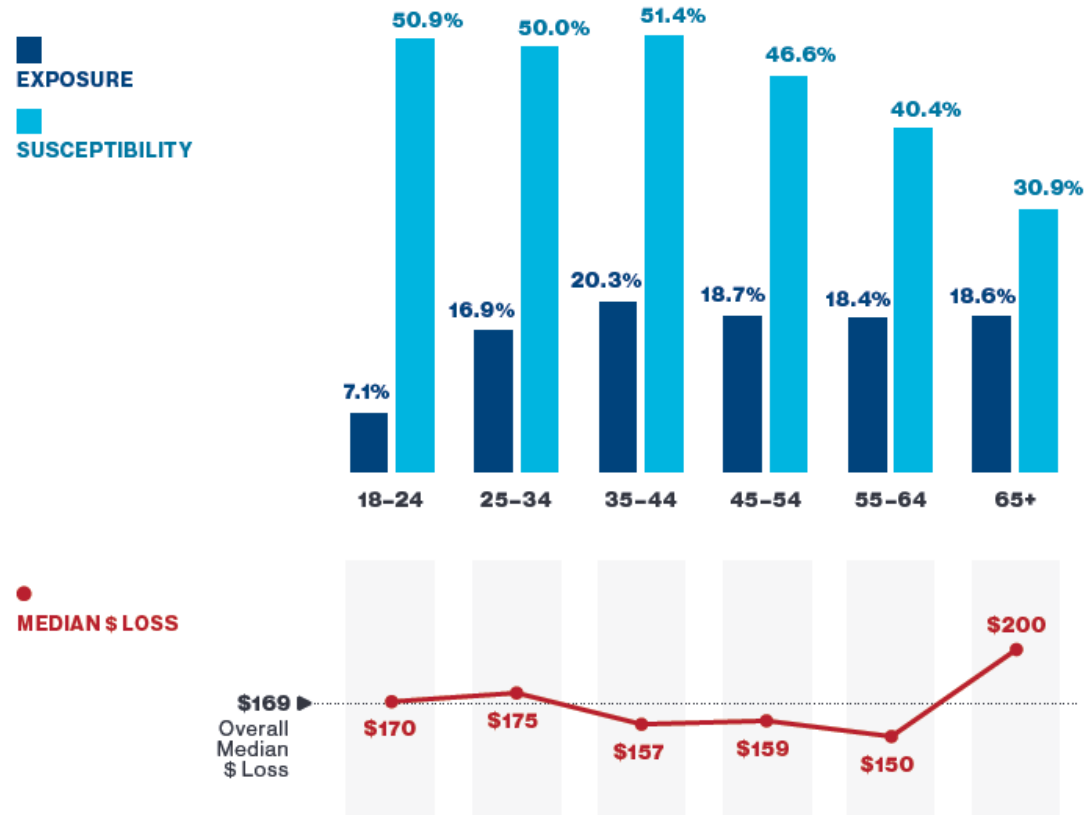
TABLE 2

Three riskiest scam types by age

	18-24	25-34	35-44	45-54	55-64	65+
1	Online purchase scams					
2	Employment scams	Cryptocurrency scams				Travel/ vacation/ timeshare scams
3	Investment scams	Employment scams	Employment scams	Home improvement scams	Employment scams	Tech support scams

FIGURE 7

Exposure, susceptibility, and median dollar loss of all scam types by age



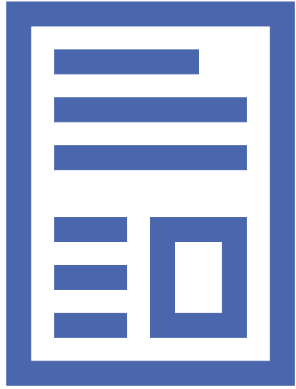
Loss of
Money by
Age

The Other Effects of Scams

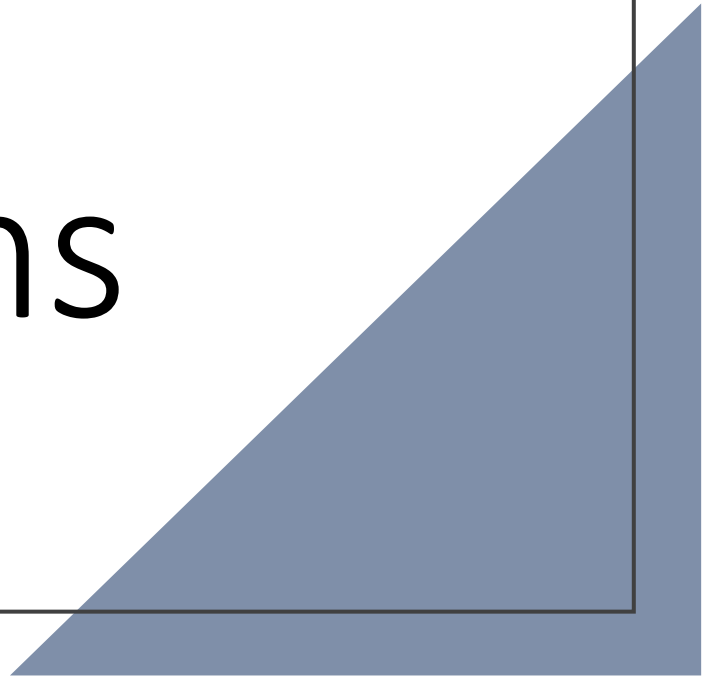
FIGURE 5

Non-financial impacts of being targeted by a scam





Reporting Scams



Where should I report a scam locally?

The image shows a screenshot of the "Fraud Report Form" from the Minnesota Attorney General's Office, headed by Keith Ellison. The form is divided into several sections:

- INFORMATION ABOUT YOU:** Includes fields for "Your Name:", "Your Street Address:", "Your City, State, Zip:", "Your Day Phone:" (with a format of () - - - - -), and "Your Cell Phone:" (with a format of () - - - - -).
- INFORMATION ABOUT THE SCAMMER (IF KNOWN):** Includes fields for "Name of Person or Entity:", "Its Street Address:", "Its City, State, Zip:", "Its Phone Number:" (with a format of () - - - - -), and "Its Website and/or Email Address:".
- HOW WERE YOU CONTACTED:** Includes a field for "How were you contacted (mail, phone, email, etc.):", a field for "Date you were contacted:", and a section for "If you were called by phone, at which phone number did you receive the call(s)?" with a format of () - - - - -. Below this is a question: "Is this telephone number registered on the National Do Not Call Registry?" with radio buttons for "Yes" and "No".
- PRODUCT OR PAYMENT INVOLVED (IF ANY):** Includes a field for "Product/Service Involved (if any):".

MN Attorney General's Office:

- ag.state.mn.us/Office/Complaint.asp
- (651) 296-3353

Your Local Police Department

Where should I report a scam nationally?


FEDERAL TRADE COMMISSION
ReportFraud.ftc.gov

Start Submit

Is your report about any of these common problems?
Don't see your problem? Choose "Something else"

- An impersonator (ex. fake government, business, love interest, grandchild)
- Job, money-making opportunity
- Phone, internet, TV service
- Health (ex. weight loss, eye care, treatment)
- Just an annoying call

- Online shopping

 **Complaint Referral Form
Internet Crime Complaint Center**

Note: Fields marked with * are required.

Victim Information

* **Name:**

Are you reporting on behalf of a business? Please select one...

Business Name:

Is the incident currently impacting business operations? Please select one...

Age: Please select one...

* **Address:**

Address (continued):

Suite/Apt./Mail Stop:

* **City:**

County:

* **Country:** Please Select One...

State: [None]

* **Zip Code/Route:**

* **Phone Number:** numbers only (1112223333)

* **Email Address:** jdoe@email.com

Business IT POC, if applicable: Name, Email, Phone number, etc.

Other Business POC, if applicable: Name, Email, Phone number, etc.

Got feedback? Tell us what you think.

Federal Trade Commission

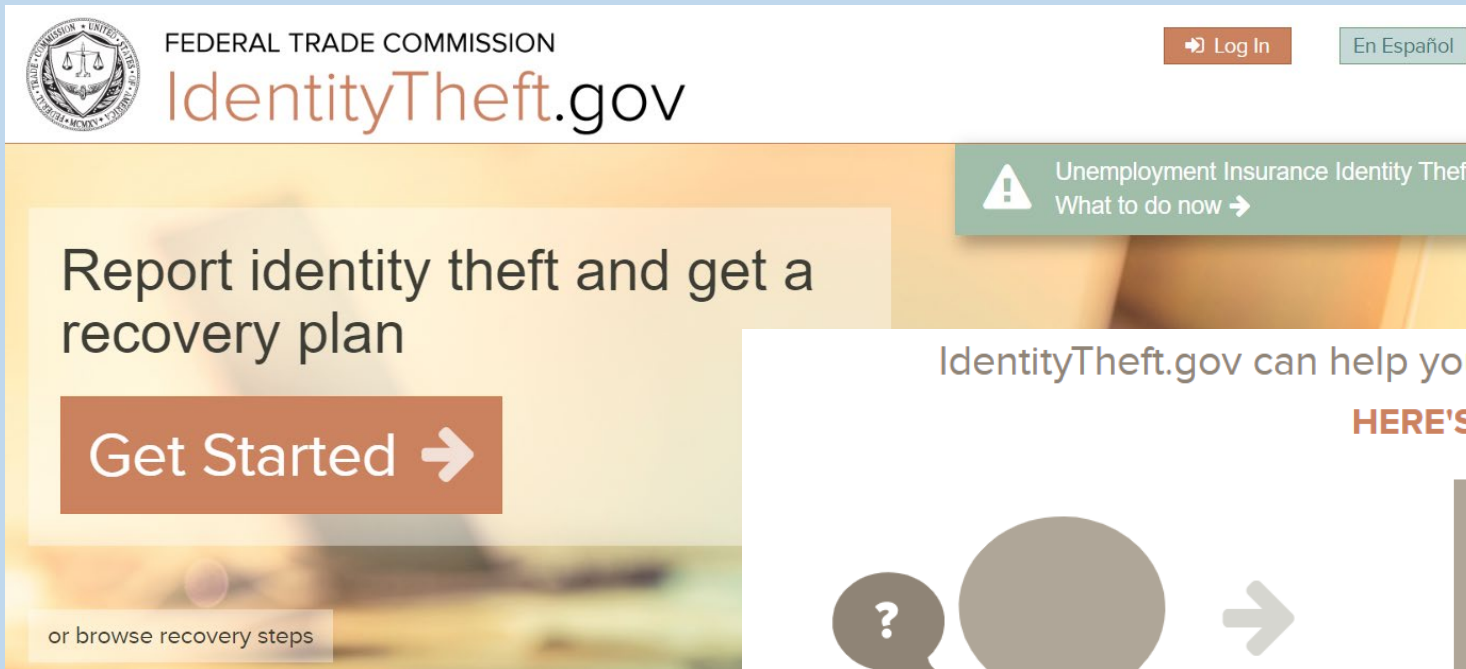
- 1 (877) 382-4357
- 1 (877) FTC-HELP
- ReportFraud.ftc.gov

Internet Crime Complaint Center

- complaint.ic3.gov

What do I do after my information is stolen?

Go to: **IdentityTheft.gov** (NOTE: make sure it is the “.gov” website!)



The screenshot shows the top of the IdentityTheft.gov website. On the left is the Federal Trade Commission logo. To its right, the text reads "FEDERAL TRADE COMMISSION" and "IdentityTheft.gov". Further right are "Log In" and "En Español" buttons. Below the header is a green banner with a warning icon and the text "Unemployment Insurance Identity Theft What to do now →". The main content area features a large orange box with the text "Report identity theft and get a recovery plan" and a "Get Started →" button. Below this is a smaller box with the text "or browse recovery steps".

IdentityTheft.gov can help you report and recover from identity theft.

HERE'S HOW IT WORKS:



Tell us what happened.

We'll ask some questions about your situation. Tell us as much as you can.



Get a recovery plan.

We'll use that info to create a personal recovery plan.



Put your plan into action.

If you create an account, we'll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.

FIGURE 7

Other factors that affect the likelihood of losing money



FACTORS THAT DECREASE RISK

Asking questions when unfamiliar with something

Believing individuals can influence and empower their own lives

Believing government institutions get their authority from individuals

Tending to be skeptical when dealing with new situations



FACTORS THAT INCREASE RISK

Feeling financial distress

Feeling lonely

Panicking during stressful situations

Findings suggest that there are other protective factors that can reduce the incidence of losing money.

Protect Yourself and Others

