Banking locally

EVER AFTER

IS KEEPING YOUR INFORMATION SAFE

INTERNET FRAUD—SENIORS AND TEENAGERS

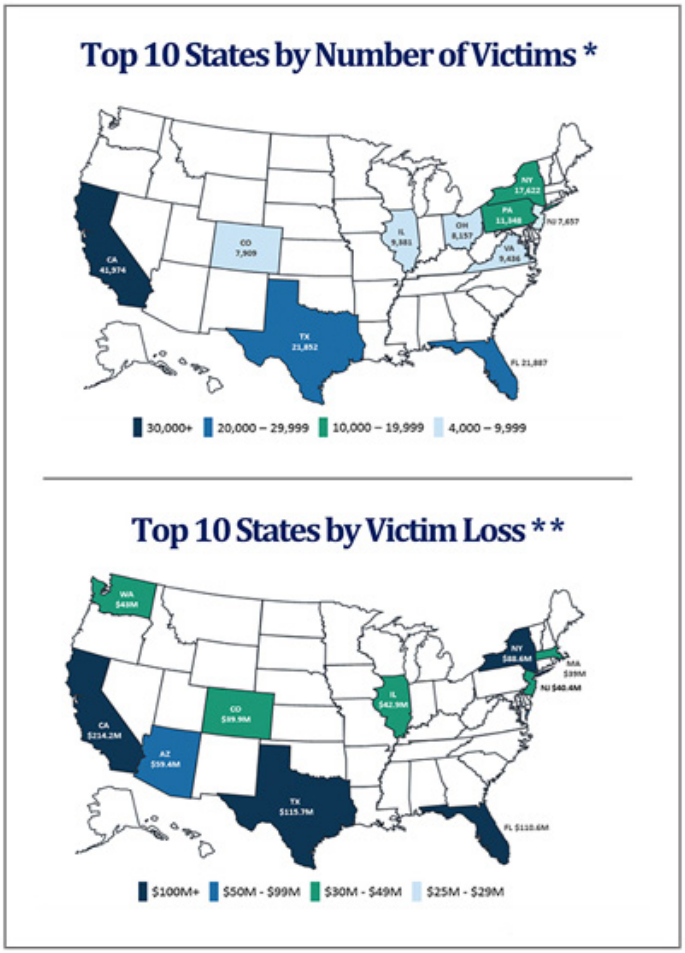
Fraud is a significant concern in today's technology-infused environment, but many of us live without thinking about fraud and its impacts every day. However, there are few things worse than fraud being perpetrated against those less aware of potential threats, including youth and senior citizens. The FBI's Internet Fraud Complaint Center reports that the incidence of fraud attempts occurs more frequently than you might expect against both those under 20 years old and over 60 years in age. The biggest difference, not surprisingly, is that those over 60 often have higher financial assets, thus, the reported losses are also higher.

2017 VICTIMS BY AGE GROUP

	VICTIMS	
AGE RANGE	TOTAL COURT	TOTAL LOSS
Under 20	9,053	$8,271,311
20-29	41,132	$67,991,630
30-39	45,458	$156,287,698
40-49	44,878	$244,561,364
50-59	43,764	$275,621,946
Over 60	49,523	$342,531,972

Source: FBI Internet Fraud Complaint Center (2018). Internet Fraud Report.

Additionally, FBI research and analysis finds that the frequency and size of various fraud types are also disproportionately higher in certain parts of the country, especially on the coasts and near borders. As a result, youth and senior citizens in California, Arizona, Colorado, Texas, Illinois, Ohio, Florida, Virginia, Pennsylvania, New Jersey, New York and Connecticut should be particularly on the look-out, though individuals in other states will want to also be diligent when it comes to preventing and rectifying internet fraud against vulnerable age groups.



* Accessibility description: image depicts the United States, with the top ten states (based on reported victims) highlighted. These include California (41,974), Florida (21,887), Texas (21,852), New York (17,622), Pennsylvania (11,348), Virginia (9,436), Illinois (9,381), Ohio (8,157), Colorado (7,909), and New Jersey (7,657).

* *Accessibility description: image depicts the United States, with the top ten states (based on reported victim loss). These include California ($214.2M), Texas (115.7M) Florida ($110.6M), New York ($88.6M), Arizona ($59.4M), Washington ($43M), Illinois ($42.9M), New Jersey ($40.4M), Colorado ($39.9M), and Massachusetts ($39M).

Insights for Senior Citizens

The American Association of Retired Persons (AARP) has found that the most common scams against the elderly include:

- Phony lotteries and sweepstakes seeking upfront fees to enter or collect.
- Government impostors posing as representatives from Social Security and Medicare.
- The grandparents' scam, in which a grandchild is supposedly in deep trouble and in need of financial assistance.
- Offers for free or discount medications (including anti-aging drugs) or medical equipment.
- Credit card fraud and investment schemes.

AARP offers the following suggestions for limiting the possibility of your parent being scammed:

- Set up online access to your parents' bank and credit card accounts to keep an eye out for unusual monthly charges, big and small.
- Unlist your parents' phone number, or replace the landline with a cell phone, which is less likely to be called by scammers.
- Put your parents' addresses on opt-out lists with the Data & Marketing Association (DMA). Once done, legitimate vendors won't send junk mail, and parents will know that what arrives is likely from scammers. That mail should be reported to the U.S. Postal Inspection Service.
- Check your parents' credit reports at AnnualCreditReport.com to ensure that fraudulent new accounts haven't been opened in their names.
- If these suggestions aren't enough or parents will not heed your warnings, call the AARP Fraud Fighter Call Center toll free at 800-646-2283.

Insights for Children and Young Adults

You'll want to be on the look-out for frequent scams aimed at children, including the "free trial offer," with the fine print of these scams including terms stating that after the trial period, you'll be paying for the product every month. Other examples include fake Wi-Fi hotspots; social media and email messages indicating you've won an expensive prize or should enter a contest to win an expensive prize; and bogus pop-ups warning of supposed viruses and malware. The latter scam often looks like legitimate anti-virus programs.

To counter these, keep an eye on errors in offers, offers that come from another country, offers that focus on your emotions, whether it is stress, loneliness, frustration, and contests, talent searches or scholarships. Talk with your children about not clicking on links or attachments, limiting what is purchased or viewed online, and using strong passwords and anti-virus products. Also, be sure to sign up for alerts so you know if anything questionable occurs on children's accounts, and review your online statements regularly. Inform children with mobile devices not to answer unsolicited text messages asking for information. Similarly, share that downloading apps can lead to fraud if children or teens are not careful. Always take time to monitor your child's internet and mobile phone use. You'll have a better sense for warning signs to be alert to and this can provide the basis for better discussions with your kids.

If internet fraud takes place, be sure to report the incident as soon as possible. Also, change passwords on all accounts, and continuously check financial accounts for any erroneous charges, new inquiries or accounts you did not authorize or establish. Taking these small steps can have a major impact on your financial health, as well as the safety of your child or parent.

Top Resources

Below are several resources which offer additional information about internet fraud and its impact on seniors and teens.

- Millennials and Internet Fraud*
- Protecting Kids Online*
- Avoiding Fraud among Seniors*
- Talking Points for Adult Children and their Parents*

*You will be linking to another website not owned or operated by the bank. We are not responsible for the availability or content of this website and do not represent either the linked website or you, should you enter into a transaction. You are encouraged to review the privacy and security policies which may differ from ours.