

2023 STATISTICS



\$12.5 Billion

Losses in 2023



2,412

Average complaints received daily

2021
2019
2018
2017
2016

758,000+

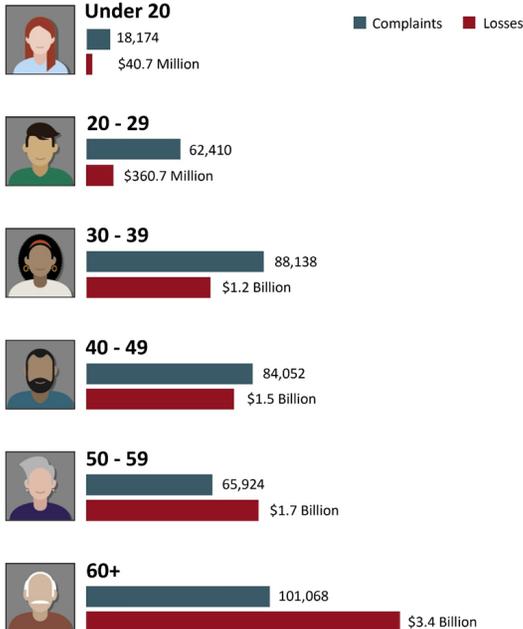
Average complaints received per year (last 5 years)



Over 8 Million

Complaints reported since inception

IC3 Complaints By Age Groups



REPORT IT!

If you, or someone you know, is a potential victim of internet fraud, file a complaint with the IC3.

www.ic3.gov

Filing tips:

- Retain original records: emails, letters, checks, receipts, shipping documents, etc.
- Financial transaction information.
- Information used by the criminals such as bank accounts, addresses, e-mails, websites, and phone numbers.

Contact financial institutions to safeguard accounts, and credit bureaus to monitor your identity for suspicious activity.

Public Service Announcements And Industry Alerts

The IC3 reviews and analyzes data submitted through its website, and produces intelligence products to highlight emerging threats and new trends. PSAs, Industry Alerts, and other publications outlining specific scams are posted to the IC3 website.

www.ic3.gov



U.S. Department of Justice
Federal Bureau of Investigation
Cyber Division



INTERNET CRIME COMPLAINT CENTER

www.ic3.gov

A LOOK INTO THE IC3

Mission of the IC3

The mission of the Internet Crime Complaint Center (IC3) is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet facilitated criminal activity and to develop effective alliances with industry partners. Information is processed for investigative and intelligence purposes for law enforcement and public awareness.

IC3 Complaints

The complaints submitted to the IC3 cover an array of Internet crime including theft of intellectual property rights, computer intrusion, economic espionage, online extortion, and international money laundering. Numerous fraud schemes such as identity theft, phishing, spam, reshipping, auction fraud, payment fraud, counterfeit goods, romance scams, and non-delivery of goods are reported to the IC3.

Elder Fraud

The Elder Abuse Prevention and Prosecution Act was signed into law in October 2017 to prevent elder abuse and exploitation and improve the justice system's response to victims in elder abuse and exploitation cases. As a response to the increasing prevalence of fraud against the elderly, the Department of Justice (DOJ) and the FBI partnered to create the Elder Justice Initiative. Elder Fraud is defined as a financial fraud scheme which targets or disproportionately affects people over the age of 60.

The IC3 is the FBI office responsible for receiving Elder Fraud complaints. In 2023, over 101,068 victims over the age of 60 reported losses of almost \$3.4 billion to the IC3. This represents an 11 percent increase in losses over losses reported in 2022. Because age is not a required reporting field, these statistics only reflect complaints in which the victim voluntarily provided their age range as "Over 60".

Internet Crime and the IC3

As technology evolves, so do the many methods used to exploit technology for criminal purposes. Nearly all crime that once was committed in person, by mail, or over the telephone can be committed over the Internet. The criminal element is empowered by the perceived anonymity of the Internet and the ease of access to potential victims. Criminals use social engineering to prey on their victims' sympathy, generosity, or vulnerability. The IC3 was designed to help address all types of Internet crime through its complaint system.

TRENDS

Business Email Compromise

In 2023, the IC3 received 21,489 Business Email Compromise (BEC) complaints with adjusted losses over \$2.9 billion. BEC targets both businesses and individuals performing transfers of funds, and is most frequently carried out when a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers.

Confidence Fraud / Romance Scams

Confidence/Romance scams encompass those designed to pull on an individual's "heartstrings". In 2023, the IC3 received reports from 6,740 individuals over 60 who experienced almost \$357 million in losses to Confidence/Romance scams. Grandparent Scams also fall into this category. In 2023, over 200 complaints from those Over 60 reported Grandparent scams, with approximate losses of \$2.3 million.

Investment

Investment fraud involves the illegal sale or purported sale of financial instruments. Examples of investment fraud include advance fee fraud, Ponzi and pyramid schemes, fraudulent crypto scams, and market manipulation fraud. 39,570 Investment victims reported Investment scams in 2023, with losses over \$ 4.5 billion. Of that loss, over \$ 3.96 billion involved cryptocurrency investments. Crypto-investment scams saw unprecedented increases in the number of victims and the dollar losses to these investors. Many victims have assumed massive debt to cover losses from these fraudulent investments and the most targeted age group reporting this type of scam are victims ages 40 to 49.

Ransomware

Ransomware is a type of malicious software, or malware, that encrypts data on a computer, making it unusable. A cyber criminal holds the data hostage, or threatens to destroy the data or release it to the public, until the ransom is paid. If the ransom is not paid, the victim's data remains encrypted. In 2023, the IC3 received 2,825 complaints identified as ransomware with adjusted losses of more than \$59.6 million.

Tech Support Fraud/Government Impersonation

Impersonation scams defraud thousands of individuals each year. Two categories of fraud reported to IC3, Tech/Customer Support and Government Impersonation, are responsible for over \$1.3 billion in losses. Call centers overwhelmingly target older adults, with devastating effects. Almost half the complainants report to be Over 60 (40%), and experience 58% of the losses (over \$770 million).

Cryptocurrency

Once limited to hackers, ransomware groups, and other denizens of the "dark web," cryptocurrency is becoming the preferred payment method for all types of scams – SIM swaps, tech support fraud, employment schemes, romance scams, even some auction fraud.

The use of cryptocurrency is extremely pervasive in investment scams, where losses can reach into the hundreds of thousands of dollars per victim. The IC3 received 69,468 complaints in 2023 reporting some type of crypto use. Losses from these complaints exceeded \$5.6 billion.