

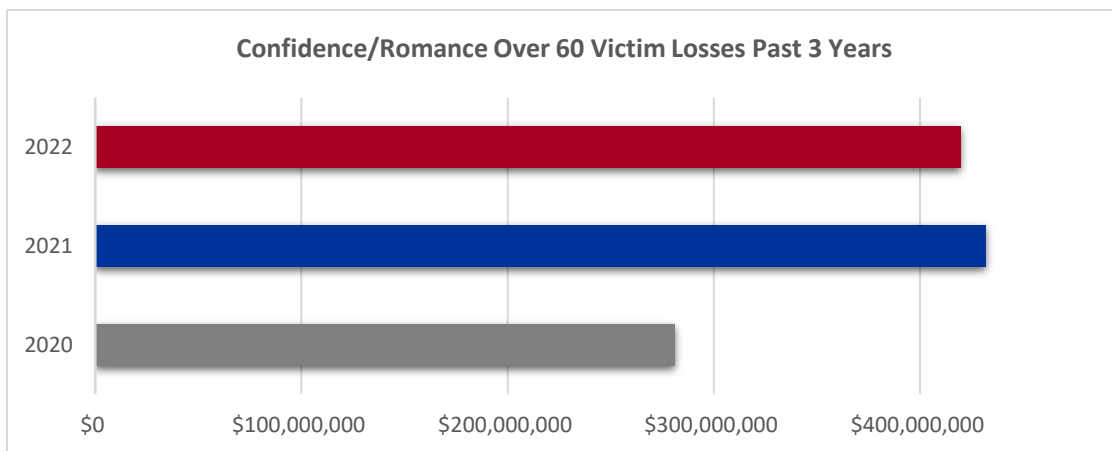
Confidence/Romance Scams



Confidence/Romance scams encompass those designed to pull on a victim's "heartstrings". In 2022, the IC3 received reports from 7,166 victims over 60 who experienced almost \$419 million in losses to Confidence/Romance scams.

Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and confidence. The scammer uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim. The criminals who carry out Romance scams are experts at what they do and will seem genuine, caring, and believable. The scammer's intention is to quickly establish a relationship, endear themselves to the victim, gain trust, and eventually ask for money. Scam artists often say they are in the military, or a trades-based industry engaged in projects outside the U.S. That makes it easier to avoid meeting in person—and more plausible when they request money be sent overseas for a medical emergency or unexpected legal fee.

Grandparent Scams also fall into this category, where criminals impersonate a panicked loved one, usually a grandchild, nephew, or niece of an elderly person. The loved one claims to be in trouble and needs money immediately. In 2022, almost 400 victims over 60 reported Grandparent scams, with approximate losses of \$3.8 million.



Extortion



Extortion occurs when a criminal demands something of value from a victim by threatening physical or financial harm or the release of sensitive data. Extortion is used in various schemes reported to the IC3, including email extortion attacks, hitman schemes, government extortion, and sextortion. In 2022, over 4,200 victims over 60 reported incidences of extortion, with losses over \$15.5 million.

Almost half of extortion victims over 60 reported to be victims of sextortion. Most believed they were in a relationship with the victim and shared sensitive photos or information which were then later used to sextort them.