Income scams: big promises, big losses

When the job market is tough, scammers target people who are looking for work or trying to bring in extra income. Economic conditions caused by the COVID-19 pandemic may have created ideal conditions for these scams to proliferate. In fact, the volume of reports to the FTC about income scams reached the highest levels on record in the second quarter of 2020.1

These income scams take many forms. Looming large are phony job offers involving fake checks. Schemes that promise to teach you insider secrets to start your own business are part of the mix, too, as are investment scams promising high returns. Chain letters and pyramid schemes are also popping up. People have reported losing about $610 million from income scams since 2016, with nearly $150 million reported lost in the first nine months of 2020 alone.

Roughly one in three income scam reports is about phony job offers with a fake check as part of the ruse. Sometimes these scams start with an unexpected email about a job. For example, some college students have reported getting messages from someone impersonating their school’s career services office. Other people have reported that the scam started after they applied for a job or posted a resume online. After a speedy hiring process, people get a supposed paycheck to deposit. But there’s always a plausible explanation for why they can’t keep all the money. Scammers tell people hired as “mystery shoppers” to buy gift cards as they evaluate a retailer (the scammers get the gift card PIN numbers, of course). People hired as “virtual personal assistants” are told to send some of the money to a supposed supplier of home office equipment. Other people have even reported that their so-called boss told them to use some of the funds to buy gift cards for co-workers sick with COVID-19.

These scams work because banks have to make funds from deposited checks available within a day or two, but it can take weeks to uncover a fake. When you see the funds in your account, parting with some of the money may feel risk-free. But when the fake check ultimately bounces, the bank will want you to pay back the funds. The median reported loss on fake check job scams is $2,300,2 and adults in their 20s are more than three times as
likely to report a loss on a fake check job scam than other age groups.³

Another common tactic income scams use is making false claims about likely earnings from starting your own business. Business opportunity scammers promise attractive incomes to trick entrepreneurial people into buying bogus marketing services, training, or coaching programs. But despite testimonials that flaunt lavish lifestyles, their “proven systems” just don’t work. People have reported that some scammers are even invoking the pandemic as part of their pitch in offering work-at-home “opportunities.” But these opportunities frequently add up to huge losses. In fact, the median individual loss people report on business and work-at-home opportunities is $3,000, and for people in their 60s and 70s, the reported median loss is four times higher.⁴

Drumming up interest in investments is another lucrative tactic scammers deploy. Many investment seminar cons work by promising to teach people how to earn high returns on things like trading online or investing in real estate. But people report losing more on these scams than on any other fraud: the reported median individual loss is over $16,000. People in their 50s and 60s are more likely than other age groups to report losing money on these cons,⁵ and their reported median individual losses are nearly $24,000.

Some income scams put people to work as unwitting accomplices in another scam, costing people their time and effort. People report being hired on a 30-day probationary period, with titles like “logistics manager.” The scammers tell them their job is to receive and reship packages. What they don’t know is that they’re reshipping items bought with stolen credit cards. And after their probationary period ends, the scammers simply cut off communication without ever paying the person.

Another variety is the pyramid scam. That old scam got new life by using novel names, like “blessing looms,” “circle games,” and “sou-sous.” A sou-sou is a collective savings club with historic roots in West Africa and the Caribbean. In a real sou-sou, money is rotated within a family or close-knit group, and everyone gets back what they contribute. Fake sou-sous, on the other hand, are pyramid schemes or chain letters. Like so-called blessing looms, they claim you’ll multiply the money you put in. But unlike a real sou-sou, payouts depend on recruiting new members – like family and friends. People typically lose all the money they invest.

While reports of fake sou-sous by any name are still relatively low, they increased sharply starting in the second quarter of 2020,⁶ and nearly 40% of people who reported said they heard about the supposed opportunity on social media.⁷

It is clear that income scams take many different forms, but they share some tell-tale signs. Keep these tips in mind to avoid income scams:

- Take your time. Avoid high-pressure sales pitches that require you to get involved now or risk losing out.
- Be skeptical about “success stories” and testimonials. Glowing stories could be fake and online reviews may have come from made-up profiles.
- Don’t bank on a “cleared” check. If you’re told to send some of the money or buy gift cards, you can bet it’s a fake even if you see the money in your account.
- Do your research. Search online for the company’s name plus words like review, scam, or complaint.

To learn more, visit ftc.gov/incomescams. If you spot a scam, report it to the FTC at ReportFraud.ftc.gov.
In Q2 2020, 11,879 income scams were reported, a 70% increase from reports captured in Q2 2019. In total, 29,419 income scams were reported directly to the FTC in 2020 through Q3, compared to 26,719 in all of 2019. These figures do not include the complaints collected by other organizations that contribute to Sentinel. Counting all reports to the FTC or any Sentinel data contributor, there were 44,274 income scam reports in 2020 through Q3 and 52,837 such reports in all of 2019. Income scams are defined in this Spotlight as frauds reported directly to the FTC classified as business and work-at-home opportunities, job scams and employment agencies, pyramids and multi-level marketing, investment seminars and advice, stocks and commodity futures trading, art, gems and rare coin investments, and miscellaneous investments. Additionally, reports about fake check scams that were identified through a keyword analysis as involving a job or other income opportunity are included.

The median individual reported dollar loss figures provided in this Spotlight are based on reports directly to the FTC for a robust and recent time period, January 2018 through September 2020.

From January 2018 through September 2020, 83% of income scam reports included age information. This age comparison is normalized based on the number of loss reports per million population by age during this period. Population numbers were obtained from the U.S. Census Bureau Annual Estimates of the Resident Population for Selected Age Groups by Sex for the United States (June 2020).

See endnote 2. The median individual dollar loss on reports classified as business and work-at-home opportunities submitted by consumers ages 60-79 was $12,000.

Reports of fake sou sou scams increased from an average of less than one report per quarter from Q1 2017 through Q1 2019 to 47 reports in Q2 2020 and 191 reports in Q3 2020. These scams were identified through keyword analysis of the narratives provided in income scam reports. Reports about multi-level marketing companies (MLMs) and pyramid schemes of all types doubled in the second quarter.

Reports in which the consumer heard about the fake sou sou on social media include income scam reports where the method of contact was specifically identified as social network, and reports where the method of contact was not specified, specified as internet, or consumer initiated contact, if the comments field also included mention of Facebook, Instagram, LinkedIn, Pinterest, Reddit, Snapchat, TikTok, Tumblr, Twitter, or YouTube.