



Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • December 2018 • www.consumer-action.org

SCAM GRAM is Consumer Action's monthly e-newsletter alerting you to the dirtiest players in the world of tech fraud, credit card scams, ID theft and general con-artistry. Don't be fooled by liars, cheats and crooks—wise up with SCAM GRAM!

Teaching student debt relief scammers a lesson

Repeat racketeer Tuan Duong is under Federal Trade Commission (FTC) scrutiny for promising "100% customer satisfaction" in reducing or even eliminating the student loan debt of those who signed up with any of the many companies he created to separate debtors from their money. Duong's (temporarily halted) debt relief scam isn't his first rodeo; in 2015, the FTC sued the prolific profiteer over mortgage relief scams (and forbade him from advertising debt relief products). Not to be dissuaded, Duong created three parent corporations—Impetus Enterprise, Inc., Fig Tree & Co., LLC and Noel Solutions, LLC—to offer his deceitful student debt relief. From there, he branched out and "also did business as" a plethora of misleadingly-titled student aid groups (created under the parent companies), including (but certainly not limited to) Aiding Student Relief, Aiding Student & Teacher and Aiding StudentS & TeacherS. (See what Duong did there? He pluralized it! It's safe to assume Duong never took out a loan for a creative writing class.) Unfortunately, those who fell for Duong's student loan scheme ended up paying \$500+ in illegal fees and "failed to obtain debt forgiveness or monthly payment reductions," according to the FTC's [complaint](#) (which is a prerequisite to suing the socks off Duong, yet again). Duong is not the only scammer the FTC is investigating—winter is coming for shady student debt relief operators across the country as the FTC investigates them en masse through its cleverly titled Operation Game of Loans. If you're looking for loan forgiveness, check out your *legitimate* options through our *Consumer Action News* edition [Repaying your student loans](#) (natch). And heed the FTC's advice: "If anyone promises quick student loan forgiveness or asks you to pay in advance for help with your student debt," it's a scam and you should immediately [report it](#). (Don't hesitate: A recent FTC study [revealed](#) that, unfortunately, the hardest hit—minority consumers—are also the ones underreporting fraud.)

Wildfire survivors: Don't get burned

The last thing Californians grappling with increasingly destructive and widespread wildfires need to worry about are the wolves circling, waiting to pick off the survivors. OK, that analogy may be a bit dramatic, but scammers are certainly looking to prey on those trying to rebuild. They do this after hurricanes; they do this after earthquakes; and they're doing it now (in some very creative ways). In addition to contacting homeowners, pretending to be insurance commissioners and home repair contractors (the usual), hucksters are [emailing](#) employees while posing as CEOs and business owners and asking for donations to help "clients or colleagues" impacted by the fires. And it doesn't stop there. Con artists are: calling and claiming to be fundraisers with local firefighter or EMS departments; promoting fraudulent crowdfunding accounts (and representing various odd "charities"); and phoning West Coast residents, impersonating the insurance or law enforcement agents who work to cross names off missing persons lists (which leads to asking for personal information, which they then use to commit identity theft). Opportunistic Golden State grifters also benefit from rental scams (since those who have lost their homes en masse need places to live) and other seemingly innocuous offerings like debris removal and cleanup services. Wildfire isn't the only thing that spreads like, well, wildfire—information does too, so check out the FTC's guide on [Picking up the pieces after a wildfire](#) (and forward to that friend of yours who moved to Cali post-college).

Shop around

This is the sale that never ends. Yes, it goes on and on, my friennnnnd! Just in time for holiday shopping, the non-profit group Truth in Advertising (TINA.org) [released a study](#) on deceptive "anchor pricing," or, in layman's terms, that awesome "Won't last!" BOGO sale that you just can't pass up. These "sale" prices aren't much of a steal to begin with, as it turns out, since so many items are perpetually "on sale." For over six months, TINA.org followed the prices of clothes, shoes, handbags and the like at a number of national outlet stores and discovered that the "sale" prices *were* the prices, since the items *never* sold at the advertised "regular" prices. As TINA.org points out, this is "a misleading marketing ploy that is incredibly effective at tricking consumers to stop their search for the best deal, and results in consumers paying more than they necessarily need to." Don't fall for it.

The secret's out. Either this "sister" has a really bad case of middle child syndrome or she's *still* angry about that bridesmaid dress you made her wear, because she's [unleashed](#) a particularly obnoxious tirade. If you're a social media user, you've probably seen it. It starts: "The Secret Sister Gift Exchange is back! I'm looking for six women who would be interested in a pre-holiday gift exchange. You only have to buy one \$10 gift..." One gift turns into many, they claim, but don't buy it. Secret Sister is a classic pyramid scheme, and the further down the gift-receiving line you are, the fewer gifts you get back (often enough, not even a lump of coal in your stocking). And chain letters like this aren't just incredibly annoying; they're illegal as well. A final reason to ignore Secret Sister (and any gift exchange schemes like her): "Your friends will hate you," as *IndyStar* points out, for bombarding them with nonsense during the busiest time of the year.

There's no such thing as a free...cruise? We get it: You're standing in that never-ending line at another big-box store, presents piled high in your rickety cart, the child beside you having a meltdown, the grumpy man in front of you slowly paying the cashier in quarters, and all you can think of is reclining on a cruise ship with a piña colada in hand, the warm sun hitting your shoulders and the breeze flowing through your hair. But no matter how much you've spent on holiday gifts or how stressed you are, remember: There's no such thing as a free cruise. Even passengers who think they've earned it by listening to a million sales pitches and attending those awful timeshare presentations "often report dismal cruise conditions and ships that lack common

amenities like air conditioning," according to the National Consumers League, who wrote an excellent [piece](#) on knowing when to cruise past that "too good to be true" vacation offer.

Tips!

● **Not all who wonder are lost.** Say you're using Google Maps to find that hot new restaurant for date night. You're driving around in circles, and your date is getting antsy, so you call the place to find out if they're *behind* the alley and in the tree or *under* the tree and above the alley (these restaurants keep getting trendier and trendier). You think you're talking to a host who asks you for your reservation information, but the convo takes a turn for the weird(er) when he also asks about your address and bank account info. Congratulations: You've just been exposed to a Google Maps scam! How? Anyone can submit changes to the service's business listings, even crooks, who now use the feature to insert their personal phone numbers in place of legit business numbers. Google says it's working quickly to address the issue, which has predominantly been [reported](#) overseas, but, as with all new and novel scams, could be heading your way fast.

● **Freeze—another breach.** This month saw two major data breaches—both due to security flaws in online systems. The companies breached? The U.S. Postal Service (impacting 60 million people) and the Marriott Starwood hotels (impacting a whopping 500 million). A USPS flaw allowed anyone with an online account to view (and, in some cases, modify) others' accounts, while investigators believe Chinese spies breached the Starwood system to get info on government officials and other persons of interest. While we're all sick and tired of hearing that another breach has occurred, it's important to keep on top of these things and take action if you think you may have been impacted, in order to avoid becoming a victim of identity/financial theft. Here's [one way](#) to be safer.

● **Under wraps.** This holiday season, you may pay dearly for the gifts you order online if you're not careful to utilize secure shopping practices. The consumer hotline network Call for Action [lists](#) some of the year's biggest cybershopping fails, including whipping your credit card out for websites that don't include the 'S' (for "secure") in HTTPS, failing to clean your online cart (and clear your cookies), and not updating your antivirus software and passwords regularly. Perhaps most interesting, the group points out that since "most websites and apps today contain technologies that track what visitors are reading and viewing, including across other websites and apps," you run the risk of anyone who uses your computer or smartphone seeing ads (even on, say, your Facebook page) for that super thoughtful present you spent so much time researching for them (and thereby ruining the surprise). Oh, brave new world!

● **Game on.** Sports enthusiasts eager to check out an NFL game in the lead-up to the Super Bowl (it's Feb. 3 this year...you're welcome) should be careful to buy tix from reputable sites. One way to know? If a seller is [accredited](#) with the Better Business Bureau and [listed](#) as a member of the National Association of Ticket Brokers, it's game on. Avoid buying from scalpers outside the stadium; they're usually selling lookalike "tickets" that won't even get you through the gate. Need to resell your ticket? The safest way is to call the organization hosting the sporting event and ask how they recommend doing so (don't just throw it up on Craigslist). Finally, if you want to score tickets to the big game in Atlanta this year, know that ticket brokers are required by law to register with the state. This works in your favor, since you can verify a broker's license [here](#) (under "search for a licensee").