# Scam Gram!

*Keep the sharks at bay*

**A Consumer Action News Alert • December 2017 • 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!

## *Coal in your cyber stocking*

Let Santa give you gifts the old-fashioned way (down the chimney), and think twice about any gift exchange coordinated through social media, even if a friend is the one prompting you to join. Two of these types of scams are floating around Facebook, and both could reveal your home address to crooks, cause you to lose money, or worse. The first is a "Secret Sister" gift exchange. You'll be getting less than coal in your cyber stocking if you fall for this one. The scam invites women to invite six people to each snail mail a $10 gift, promising the senders they'll ultimately receive 36 gifts in return. According to the Better Business Bureau (BBB), this cutesy con constitutes a pyramid scheme, and "pyramid schemes are illegal either by mail or on social media if money or other items of value are requested with assurance of a sizeable return for those who participate." As such, "participants could be subject to penalties for mail fraud." Ho ho nooo! The second scam might be a bit more enticing to those of us struggling to stay sane in the face of cold weather, crowded malls and crazy relatives: The "Wine Exchange" operates the same way—send one bottle and get a whole bunch back. The same BBB cautions apply here too, with an additional factor: The USPS, UPS and FedEx have strict rules about sending booze through the mail (the USPS doesn't allow it at all), so you might inadvertently get busted on both counts if you send your best bottle of red to a stranger. (It's also worth mentioning that those participating in these schemes have reported they've received neither gifts nor vino.)

## *Not jury duty agaaaaain!*

The feds are warning the public to be aware of the tried-and-true jury duty scam, which has been around for years but has recently seen a *huge* uptick in calls. The callers threaten their victims with arrest or jail for failing to report for jury duty. (We've seen this one covered in local media in dozens of states around the country over the last month, with lots of miserable victims lamenting their losses.) If this scam seems like an obvious "hang up the phone" type situation, don't be so sure you wouldn't fall for it. Scammers

introduce themselves by the names of real U.S. marshals, judges and other government officials. Victims are describing the callers as “very, very believable,” according to U.S. Marshals, and have been taken for “amounts ranging from $500 to more than $2,000.” The scammers will also give the address of the target’s local courthouse, along with case and badge numbers. The U.S. Marshals are urging anyone contacted by these criminals to report them not only to their local U.S. Marshals Service office, but also to the Federal Trade Commission (which investigates and prosecutes all sorts of scams). And they couldn’t be clearer: “In no instance will a court official, U.S. Marshal, or other government employee contact someone and demand payment or personal information by phone or email.” The chief added that falling for the scam can be “devastating, especially during the holidays," when they could blow a hole in your holiday budget.

## *Breach blowback*

It was only a matter of time: The news is coming in that credit holders across the country are feeling the pain from September’s Equifax breach (the largest data breach in history!). Consumer reporter Ken Harney details some of the complaints from a massive class action suit that includes victims from all 50 states: A Virginia woman has “experienced multiple fraudulent charges on five of her credit card accounts”; a Mississippi man reports that criminals have applied for student loans using his identity; a Vermont woman has been hounded by debt collectors for “loans that she never opened”; and so on. If you haven’t gotten around to buttoning up your personal data, these stories should provide the impetus—after all, the breach has impacted pretty much everyone with a credit history. Our short guide on how to do so could apply to just about any breach, including the latest wrong turn by Uber, which shamefully attempted to hide its customer data loss from the public. Hackers stole personal data from millions of Uber drivers and riders last year, a fact that is just now coming to light after the ridesharing company paid the creeps $100,000 to “destroy the data, pressured them to sign nondisclosure agreements, and portrayed the ransom as a payment to test the vulnerabilities of the company’s data security systems.” (Click here for the story.) Perhaps the bad behavior will stop when legal ramifications cost these companies enough (we’re not holding our breath, though). Sixty and counting class actions have been filed against Equifax; if you’re looking to get in on the action, you can view a list of ‘em here. Shockingly, there is no national data breach notification standard. Congress has been making noises, but for now all the action is in the states.

## *Holiday hoaxes*

**Knock it off.** Consumer Action runs a consumer complaint hotline, and every month, in our *INSIDER* newsletter, we feature one complaint that’s particularly impactful. The latest is here just in time for the holidays: A consumer purchased a Coach purse that turned out to be a knock-off bag. The woman attempted to return it, only to be told that even if she sent it back at her own expense, the seller would deduct a “10% bank fee, 30% handling fee and 10% shipping fee.” If you’re planning on shelling out the big bucks for friends or family who’ve developed a taste for the finer things in life, learn from this woman’s mistake and avoid falling victim to the massive counterfeit goods “industry.” (As much as $460 billion worth of counterfeit goods were bought and sold last year alone!) How can you tell a fake? For one thing, if the price for a “luxury” item (complete with fancy logo) seems too good to be true, it probably is.

**Throw this phish back!** A sophisticated phishing attack is catching consumers who shop online through PayPal. Legit-looking emails boasting the company’s logo and originating from service(at)paypal.com confuse already-in-a-rush holiday shoppers by stating that their recent transaction cannot be verified and

claiming their password was changed. (Another less ambitious email making the rounds simply cites "changes" to the individual's account.) As is typical for phishing attempts, the emails prompt would-be victims to click on a link in order to "prevent unauthorized persons" from accessing the account (oh, the irony!). Of course, the link takes users to a mock PayPal site, where the non-eagle-eyed might enter their personal or financial information. However, if you're paying for gifts using your computer or smartphone, there is *some* good news this year: Online retail card fraud has decreased considerably since last year, as e-commerce sites have gotten better at shutting down attempts to use a stranger's credit card without their knowledge.

**Hard to grasp.** Fingerlings are the new fidget spinners. Kids are gaga for the (kind of creepy) robotic animals that latch on to your fingers and react to movements. Unfortunately, third-party seller/scammers are just as ubiquitous as the finger-things, with lots of moms shocked that they never received the packages they ordered off Amazon months ago. On the plus side, many of the moms have been able to get their money back due to Amazon's "A-to-z Guarantee" (which refunds them for all purchases made through the site). The saga is ongoing, however: While the company that makes the toys has sued hundreds of fake sellers, more pop up to replace them daily. And the toys are so hot that it's now too late to purchase them: Not only have they flown off the cyber shelves, they're largely out of stock at Toys"R"Us, Walmart and Target. Some parties are still selling them to pressured parents, however—at markups of 100 percent plus! Worse, authorities say they've seized counterfeit toys with lead in them and electronics that can catch fire. If you're fixated on "fingering" out how to get a fingerling, click here here for official retailers.

## *Tips!*

- **Baby, it's cold outside.** National Utility Scam Awareness Week was last month, and in celebration, we're covering the issue here (well, that and the fact that 'tis the season for utility scams). Electric, water and natural gas customers are getting calls from imposters who threaten to cut their heat, power, etc. off if purportedly late payments aren't made immediately (often through prepaid debit cards, wire transfers, gift cards and the like). According to the BBB's 2017 Scam Tracker report, the average loss for these types of scams is $500. (Unfortunately, this woman lost even more.) If you get a call demanding immediate payment, hang up, even if the call shows up on your phone as your utility company (a trick that isn't hard for a scammer to rig).

- **Five crooks a' scammin'.** Consumer credit reporting agency Experian has outlined "five seasonal scams that can wreck your holidays." There are, of course, online shopping and email scams (which we've covered in detail in the sections above). Then there's holiday travel, employment and charity scams, which may not be what immediately come to mind when you think of the holidays, but typically target those looking to visit family, earn some extra cash (perhaps for gifts) and help people who are less fortunate around the holidays. Learn more here.

- **Problems with authority.** If you've spent any time reading this newsletter, then you know that IRS scams are some of the most pervasive. (We cover them, like, every other month. Really, scammers, it's getting old!) The good news: Telecom companies can now block incoming calls impersonating IRS numbers (and other annoying robocalls). The bad news: This month there's another W-2 email phishing attack (that appears to come from the IRS) to cash in on employees' personal/tax information. The IRS says that the sender poses "as a company executive, school official or someone of authority within the

organization." Often, the emails start with "Hey, you in today?" before demanding a staffer (usually an underling) email back with the entire organization's employee W-2s. If you've received some tripe like this, don't stomach it—learn how to report it here.

**Fed up with food fraud.** A reader wrote in encouraging us to warn others about food scams. He's noticed that even popular companies like Trader Joe's sell mislabeled products—for instance, grated Parmesan marketed as 100 percent cheese (with powdered cellulose listed in the ingredients). We've covered food fraud in the past but decided to do a little more digging to see what was currently "trending." To our horror, we found that even chocolate isn't safe! What's more, a new study reveals that a full 10 percent of food and drink products are "adulterated or mislabeled." If you suspect a food is mislabeled, you can contact your state's FDA consumer complaint coordinator here.

**Bogus bitcoin.** The new Cyber Unit at the Securities and Exchange Commission (SEC) has filed its first charge against the company PlexCorps, which deals in digital currency. Some companies, like PlexCorps, "go public" with what are known as "initial coin offerings," or ICOs. Consumers looking to invest in the companies can do so by buying up digital tokens or currency (cryptocurrency) like Bitcoin. Just like stock offerings, the companies often court investors with big claims: sometimes too big. PlexCorps made the mistake of promising investors they would see an outrageous 1,354 percent profit in less than a month. Of course, PlexCorps had no way of knowing if that was how things would pan out (and now it's unlikely they will). The SEC is boasting that it "acted quickly to protect retail investors from this initial coin offering's false promises." If you're investing in digital currencies, do lots of research first (and think twice), as this "industry" is still largely unregulated.

**Revenge fantasy becomes reality.** *Bloomberg* has written a fascinating story about a man by the name of Andrew Therrien, who hunted down a particularly aggressive scammer after the crook called and threatened to "rape his wife" over a non-existent payday loan debt. Criminals make millions of these "phantom debt" calls each year, complete with terrible threats like the one Therrien received. But most people don't work 'round the clock to get inside the heads of the bad guys and hunt them down. As *Bloomberg* reports, Therrien "was a bit like Liam Neeson's vigilante character in the movie *Taken*—using unflagging aggression to obtain scraps of information and reverse-engineer a criminal syndicate." Therrien's odyssey ultimately led to a Federal Trade Commission lawsuit against the criminals at the top who sold millions in fake debt. Nonetheless, authorities warn against engaging scammers, which could put you on "sucker lists" shared by scammers and result in even more calls.

**(In)secure.** The blue screen of death is back, and "tech support" scammers are employing it to trick frustrated computer users into buying fake antivirus software by the name of "Windows Defender Essentials." If your computer freezes up and prompts you to pay for the alleged Microsoft product (via a link directing you to PayPal), do not pass go; do not pay $25. Fortunately, there's a simple way to make the awful blue screen (and the malware) go away.

**Putting out fires.** Local fire and police departments are putting out fires (of the figurative variety) right and left as they send alerts out to their communities imploring them not to fall prey to scammers soliciting donations "on behalf of" their departments. Criminals across the country are using phone and email methods (and even in-person collections) to enrich themselves in the name of first responders, even going so far as to ask businesses to buy ad space to support local offices. If you're interested in *really* helping the boys in blue (or yellow? What color do firemen wear?), hang up and call the department directly (and while you're at it, report the scam).

Thanks for reading SCAM GRAM and, as always, feel free to send us your questions, comments and tips. Click here to email us.

Use our "Tell a Friend" page to let your friends know they can sign up for their own copies.

---

*Consumer Action empowers low- and moderate-income and limited-English-speaking consumers nationwide to financially prosper through education and advocacy.*

---