Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • August 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!

Phony prescription prices

It's bad enough when *scammers* call you pretending to be with your pharmacy in order to bilk you out of your money, but what about when your pharmacy defrauds you directly? A recent consumer lawsuit argues that, due to a surprisingly common practice known as the "clawback," your trusted CVS pharmacist could be charging you way more for that prescription than you're actually required to pay. Here's how it works: Pharmacies use middlemen (who have profit incentives) to negotiate the price for your pills with the drug companies on behalf of your insurance company. Most of us know what a copay is (set by your insurance company to allow you to pay a fraction of the cost for a drug or medical service). In some cases, however, the drug is actually *less* expensive than the copay. Here's an example: The drug costs $10. Your standard copay is $50. The pharmacy is advised by the middleman to charge you your full copay, and guess who pockets the $40? The middleman, who "claws back" the cash. The irony is that you likely would have paid less for the drug if you *didn't* have insurance! Sadly, pharmacists aren't required to tell you when the cash price of a drug is cheaper than your copay. According to the *Los Angeles Times*, 59 percent of pharmacists responding to a national survey reported that they were actually *prohibited* from volunteering the information! So what does this mean for the consumer? You have to ask the pharmacist about the true cost, and even then, you might not get a straight answer; only a handful of states have laws protecting honest pharmacists.

Wells on repeat

Beleaguered bank Wells Fargo, which was penalized for encouraging its employees to create millions of fraudulent bank and credit card accounts in consumers' names, is in even more hot water now. This time it's over auto insurance; specifically, unnecessary duplicate collision insurance, which the bank forced on 800,000 consumers who took out auto loans (many of whom had their cars repossessed because they didn't realize they had been signed up for it), as well as another type of insurance called guaranteed auto

(or asset) protection (GAP). GAP essentially protects purchasers in the event that, say, they "Baby Driver" off the lot and the new car (which just lost thousands in value simply by leaving said lot) is T-boned by a truck. (While standard auto insurance would cover the lesser market value of the depreciated vehicle, GAP covers how much the car *was* worth just seconds before the owner took it for its first spin.) While GAP insurance is not required, auto dealers and lenders have selfish reasons for wanting you to purchase it (particularly since the coverage is added to the total auto loan amount). That self-interest is to be expected. The problem arose in Wells Fargo's case when the bank failed to refund customers (as required) their pro-rated *unused* GAP insurance money after they paid off their loans early. While this has been the latest development in the Wells Fargo saga, it's likely not the last. We'll keep you updated as the investigations, class action lawsuits and fines pile up. Oh wait, this just in: The bad news bank is now being accused of ripping off vulnerable mom-and-pop businesses. Sigh….we can't keep up.

Siphoning your SSI

Be forewarned: Some jerk is impersonating a Social Security Administration (SSA) employee and calling people nationwide from a phone number with a 323 area code. Sound familiar? Usually this imposter scam involves some lowlife pretending to be with the IRS. The playbook is similar: The criminal is trying to get you to give up your personal information. Once he has it, he'll call the SSA and change the direct deposit, address and telephone information you've got on file (no doubt to route your payments to an account he's created). We all want to get the most out of our retirement, which is why this particular scammer knows he can nab victims by telling them that they're due for a "cost of living increase," which, of course, he can facilitate. While the SSA may call you, they're more likely to send a letter, and they're very unlikely to ever request that you confirm personal information over the phone. (In the rare cases where they do, they've already corresponded with you and established a relationship, according to the agency.) Either way, we recommend you kindly hang up the phone and call the SSA back yourself to make sure you're on the line with the real deal. The SSA is advising the public to report any suspicious calls to the Office of the Inspector General at 800-269-0271 or online.

What will they think of next!?

Your dog, the spy. You never in a million years imagined that your loyal companion Fido would give your personal information to criminals. Unfortunately, Fido may have been a privacy liability since you adopted him if you tied your cell phone number, email or other contact information to the small microchip he was fitted with when you picked him up at the shelter. And if that contact info is in a publically visible (or hackable) database, scammers are just desperate enough to contact you with an alert about your pet as an opening line before attempting to "fetch" more personal/financial info.

A total eclipse of your cash. Opportunists are looking to make money off those looking to the sun during the upcoming Aug. 21 eclipse. While it's true that you could go blind if you fail to use the correct eyewear while staring at a solar eclipse, not all protective goggles are created equal. As *The Atlantic* points out: "Regular ole Ray-Bans will not protect your peepers." NASA is warning consumers that hucksters are marketing unsafe products right and left and recommends that sun-gazers stick with only those made by the companies American Paper Optics, Rainbow Symphony, Thousand Oaks Optical or TSE 17.

Playing house. We've all heard about tricksters convincing lottery players they've hit the jackpot. But a scanty scratch-off ticket is a far cry from the beloved Publishers Clearing House sweepstakes. Smart

scammers know that so many are eager to believe Lady Luck has smiled upon them that they'll go to great lengths to collect the Publishers' prize. If the real deal ever shows up at your door, however, it'll be with balloons and a giant check (whereas fraudsters will simply call or email to tell you that you've "won"—as soon as you send them money for the "fees and taxes" associated with the sweepstakes, of course). If you still think you may be that one-in-a-billion winner, you can call the Clearing House at 877-3SWEEPS (877-379-3377) and they'll let you down easy. And in case no one's ever told you, sweepstakes are designed primarily to get information about you that can be sold to marketers. How about some more junk mail as your prize?

Tips!

- **Bad for your health.** Unless you're expecting a $14,000 grant from the National Institutes of Health, you might want to hang up if someone randomly calls offering one (and asking for your credit card number, bank account info, etc. in order to deliver the moola). While this very-specific government imposter scam is new, our caveat remains the same: No government official will ever call and ask you to pay to apply for or be awarded a scholarship/grant.

- **Tried and untrue.** A company offers you a low-cost trial period before fully purchasing a product or service. Sounds straightforward and simple, right? Actually, it can be a scam, and one of such a complex nature that the Federal Trade Commission (FTC) has created a flowchart of sorts to sufficiently describe it. The infographic uses the (very real) example of a tooth whitening company that, via "deceptive claims, hidden fine-print disclosures and confusing terms," not only stripped users of stains, but also $200 a month in recurring payments. We can't even begin to describe the entire web of lies, so check out the FTC's handy visual aid here to learn what to avoid.

- **It's electric!** Our friends over at the National Consumers League (NCL) are warning the public about a recent, dramatic rise in utility imposter scams. While these types of calls aren't new, they are (unfortunately) very effective. Consumers worried that their power will be shut off (especially now, in the dog days of summer) are quick to pay up. NCL advises you take three steps to avoid becoming a sucker: Hang up the phone and call your utility company direct to confirm you owe the payment in question; never pay in a sketchy way (i.e., by prepaid card or wire transfer); and, of course, never give out your personal info to a cold caller.

- **Flip the script.** You've probably seen the type of video or audio recording gone viral: the one where a would-be victim realizes it's a scammer calling and spends the day tormenting the *scam artist* (for our amusement) instead of the other way around. The host of a podcast called "Reply All" (episodes 102 and 103) wanted to see what would happen if he took this approach *all the way*, actually traveling thousands of miles from the U.S. to India to meet the tech scammer who dialed his number. His scintillating story provides a rare insider look into how call center operations work (and if this tale's not enough for you, check out AARP's just-posted video of a tech scammer tell-all). (Oh, and be careful about engaging scammers, because people who do usually end up on "sucker lists" and become even more enticing to con *artistes*.)

- **Stay off my stuff!** The Federal Trade Commission (FTC) recently threw a competition to see who could best help consumers protect their Internet of Things (IoT), the term for the internet-connected devices that we use to do everything from monitoring our fitness and checking in from afar on the nanny to

automating our thermostats. The FTC's $25,000 award went to a developer who created a clever app called IoT Watchdog, which will help users manage the ever-increasing online devices in their homes while flagging those with security issues. We're just waiting for it to hit the market!

Sound the alarm. Knock, knock. Who's there? A salesperson at your front door claiming to be with the home security company you've hired and offering to alter or improve your current contract. If you believe him, the joke's on you. These guys aren't representing the organization you're paying to protect your property; they're with another outfit, and if you sign the contract they're pushing, you could end up paying *two* monthly bills—one to your current company and one to the fraudsters. Hot tip: If they say they've got a deal for you that's good for one day only (i.e., use pressure tactics) or claim that your current alarm company has gone out of business, tell 'em boy bye.

Grift savings plan. If you're a federal government employee, you might be contributing to the Thrift Savings Plan (TSP), which is the fed's version of a 401(k). Unfortunately, some take our humble public servants for sitting ducks; this year alone there have been multiple scams targeting TSP investors. The Securities and Exchange Commission (SEC) just filed fraud charges against one group of brokers who misrepresented themselves as government-sanctioned advisers, when in fact they were looking to siphon savings from workers by diverting them from their tried-and-true TSP plans to riskier, high-fee annuities.

Mortgage mayhem. If someone contacts you claiming that they can modify your mortgage, make sure the offer is real or you could end up like this woman, who lost her home of 30 years. It's understandable that she fell for the fraud, though, since it referenced a legitimate government mortgage modification program, HARP. The catch? She, and many others, were instructed to address their mortgage "reinstatement fees" and payments to (unbeknownst to them) criminals. As a result, the ringleader of the devastating scam became so rich off the struggling homeowners that he even created his own bombastic YouTube station, "MakeItRain TV." (If you want to know if you are really eligible for the re-fi program, visit Harp.gov, a program of the Federal Housing Finance Agency.)

War on robocalls ramps up. The FTC has launched a new initiative to crack down on obnoxious robocalls. Soon, when consumers report the calls to the government agency, it will hand that list of numbers over to the phone carriers so that they can take the ball and run with it, blocking the calls for their customers.

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.
