Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • June 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!

Both sides of the coin

If you want to listen to two young finance dudes argue over the pros and pitfalls of Bitcoin investing, click here. Otherwise, we'll sum it up for you: A lot of tech startups are promising you riches if you invest in their burgeoning projects through "initial coin offerings," where you trade your *real* money for the digital currency Bitcoin. These would-be next-big-things claim Bitcoin may soon be worth way more than your dollar and can be used on their websites, apps, etc. to purchase products and services. Beware, however, as the Bitcoin market is pretty much totally unregulated, and according to one of the aforementioned finance dudes, 99.9 percent of these tradable financial "opportunities" are also totally speculative (if not outright scams). We know, we know, Bitcoin and other "cryptocurrencies" are all the rage right now, as are "fintech" and other online ventures. But look before you leap. First, beware of any company that promises you the world. (They should be able to acknowledge that there is at least *some* risk to investing in their venture.) Second, check with the BBB to see if a business is legit before investing (keep in mind, however, that others may not have reported it as a scam yet). You can also ask the company for a written prospectus, which contains detailed info on the product/business (it's a red flag if they can't present one) and look the seller (who's asking you to invest) up on FINRA's BrokerCheck service, which tells you instantly whether a person or firm is registered, as required by law, to sell stocks, bonds and more. Finally, you can turn to a professional accountant or attorney for advice: They're paid to tell you if you're about to do something foolish. Learn more about common Bitcoin scams here.

Landlords from hell

Most of us have experienced bad landlords who take a few days to fix the leaky sink. Notorious slumlords Steve Croman and Colony Capital founder Thomas J. Barrack, however, make *those* guys look like saints. Croman—who owns 150 buildings in New York City—has for some time been under investigation by the state attorney general, who called him the "Bernie Madoff of landlords." Croman used sketchy tactics to

push low-income tenants out of his rent-regulated apartments, including (according to the tenants who created a "Stop Croman" website): setting up hidden surveillance cameras in crumbling rental properties to monitor residents so he could find an excuse to evict them; "renovating" the properties to turn them into hazardous and deafeningly loud construction sites; saddling tenants with "frivolous and bogus lawsuits"; and refusing to make repairs. According to *Gothamist*, Croman just pleaded guilty to three grand larceny counts as well as mortgage and tax fraud. Ironically, Croman's housing situation isn't looking so hot now: He'll be leaving his multimillion-dollar mansion for a year's stay in jail. But what about Thomas Barrack, you ask? Barrack, like Croman, is in hot water for his attempts to profit by pushing renters out. He, however, has been dealing in single-family foreclosures (a market that has grown exponentially since the housing crisis in 2008), buying them up with loans from big banks in order to convert them to rentals. This profit incentive leads Barrack to eject low-income renters for those who can fatten his and his shareholders' wallets, resulting in the type of dehumanizing situations detailed by the Center for Investigative Reporting (like a three-day eviction notice over less than $50 owed in rent). Don't be a terrified tenant: If your landlord reminds you of Barrack or Croman, contact your local housing or health department or sic your state attorney general on 'em!

Real relief for student borrowers

There's a booming underground industry that promises to relieve your student debt—for a price, of course. Don't buy it. Any company that's offering to help you in this arena for any cost is likely to be a fraud. Case in point: Strategic Student Solutions, which is in hot water now for telling struggling borrowers it could reduce or forgive their loans and help repair their credit for upfront fees of up to $1,200. The students-of-life soon discovered that they were in a bigger financial bind than before. "None of their payments had been put towards their student loans," reports the Federal Trade Commission (FTC), "and their credit had [of course] not been repaired." While most good things in life *aren't* free, student loan assistance through the Department of Education is the exception, so turn to them for repayment advice instead of alliterative companies like Strategic Student Solutions. (If you need help planning out how you're going to pay back student loans, check out the Consumer Financial Protection Bureau and Education Department's super-helpful Payback Playbook.) But what if the Dept. of Ed. contacts you first? Make sure it's really them. How do you know? For starters, they're not going to ask for money (we went over this one!). Don't be this woman, who was so happy to hear that the alleged agency was going to cover $25,000 of her $85,000 in debt that she was willing to pay them $500 a month in fees (as opposed to her usual $1,000 a month in student loan payments) and, at their behest, ignore her real lender's calls because the scammers would "take care" of her loans. Instead, the imposters took care of draining her pocketbook.

A not-so-quick buck

Nothing worth having... Right above this section we wrote about *student* loan relief companies that require upfront (also known as advance) fees. Fact is, *any* offer that guarantees you can get a loan by paying an upfront fee is questionable at best, and at worst, illegal. Application, processing and other "junk" fees are allowed, but typically only if they are disclosed clearly in loan documents and payable upon receiving loan approval. Our friends at the National Consumers League, who run the excellent Fraud.org, wrote an article on the boom in these guaranteed loans, which don't even pretend to require credit checks (because, why would they?).

Scam-o-meter. The FINRA Investor Education Foundation has released an online tool to help gauge whether or not that venture you're considering investing in is legit. Though it be but little (with just four questions), the scam meter is a fiercely effective way to quickly determine (based on where the investment idea originated, who is selling it, etc.) whether or not you're about to make a big mistake (like this unfortunate couple did).

Finders, keepers. Yippee! You might feel like you've hit the jackpot if you get a letter in the mail saying that the state is holding on to your unclaimed money or property, worth untold thousands. Scammers are counting on it, sending letters through the mail claiming to be with the National Association of Unclaimed Property Administrators (NAUPA). Don't get too excited, though, particularly if the letter prompts you to send money to claim money: The scammers will be keeping all of it. If you're wondering about unclaimed property, you can find out through this *real* NAUPA-endorsed website.

Tips!

- **Hablando sobre las estafas.** A new bilingual English/Spanish Federal Trade Commission (FTC) fotonovela (illustrated storybook) details the importance of not only reporting scams to the FTC (at ftc.gov/complaint), but also telling your friends and family about any you've encountered. As the fotonovela notes: "Latinos are more likely to experience fraud" (particularly of the "notario" variety, which the *Chicago Tribune* just covered in depth), but those who talk about it can alert others in their community before they become victims.

- **It's an ambush!** Scammers have set up a phone line to bilk money out of veterans who happen to misdial the Veterans Choice community-based medical program number. The fake number (800-606-8198) is almost the same as the real number (866-606-8198). The tragic genius of this scam is that the vets walk right into the trap by accidentally dialing the 800 instead of 866. They're then prompted to provide a credit card number for a $100 rebate (and the rest is history).

- **A sticky situation.** Some scammers are kickin' it old school, forfeiting the digital treachery for a simpler strategy: stealing letters placed in blue USPS collection boxes. How do they do it? By coating the mailbox drop area with a sticky substance that catches the letters on the inside of the lid. They then come to collect the contents, which can range from money to personally identifying information. It's easy to avoid this scam though: Just re-open the door and make sure your letter made it to the top of the pile.

- **Homeland hackers.** The U.S. government is concerned about a rise in attacks from hackers targeting the social media users who work for it. The tactic: spearfishing, which occurs when the computer criminals send messages to users (say, on Twitter) with links that give them an "in" to the computer system. The problem is pervasive. A recent Russian-led attack personally targeted over 10,000 Department of Defense employees on Twitter. And research shows that up to 66 percent of these types of messages are opened by the intended victims. Learn more to stay in the minority.

- **Size isn't everything.** Spending money to lengthen your telomeres (or any other part of our body) is a fool's errand. Telomeres—which cap off the ends of your chromosomes—have been causing a fuss in the pseudo-science community, which is selling the public on a bizarre bill of goods. Genetic companies offer testing and "DNA lifestyle coaching" for a price, claiming that the longer your telomeres, the longer your life. Science, however, doesn't back this up, as telomere length is determined by genetics (and longer

telomeres have actually been linked to a greater risk of various types of cancer).

What's this all aboot? It's bad enough that scammers pretending to be with the U.S. government have been contacting immigrants and threatening to deport them; now they're contacting those same immigrants and claiming to be with the *Canadian* government. Of course, the backstory is the same: The immigrant is "under investigation" and at risk of arrest or a one-way ticket home if they don't pay up. Don't believe it, no matter the alleged origin.

Shockingly, not a scam. Two legitimate organizations, Nationstar Mortgage and the Social Security Administration (SSA), are sending out surprisingly scammy-sounding letters that are, in actuality, real. The mortgage company is rebranding itself as "Mr. Cooper" in an effort to (ironically) gain the trust of consumers who (they believe) will view the ambiguous identity as a personalized representative who "always goes the extra mile." Then there's the SSA letter that leads with "You May Be Able To Save $1,608 Or More In Medicare Costs!" So many seniors reported the enthusiastic exclamation as a scam that the National Council on Aging felt obliged to put out an alert that it wasn't. Go marketing gurus!

Fewer financial frauds. Woohoo! The Department of Labor is finally rolling out a major rule to keep your financial advisers honest. Believe it or not, prior to the rule, retirement account advisers could recommend you invest in financial products that made them rich at your expense. The rule already is under attack by conservative politicians. Learn more.

When your best isn't enough. You think that if you're vigilant and make sure that the link you're clicking on is the correct URL, you won't be taken to a fake site. Unfortunately, there's a way around such precautions. Developers (and scammers) can substitute symbols for the characters in a trusted link like https://www.appıe.com/. The symbols look like the corresponding English letters. (Go on, copy and paste the Apple link into your browser and see how it works. Also click here to learn more about this devious trick.)

Crazed crackdown. The *New York Times* has published a disturbing report on how the National Guard has ruined the lives of military and ex-military members in its zeal to find and prosecute those who they claim scammed a now-defunct program called the Guard Recruiting Assistance Program. According to the paper, "Many of the accused have lost jobs or been denied military promotions, even when charges were eventually dropped. They have fallen into debt trying to defend themselves and suffered the anguish of living under public suspicion." There are real soldiers defrauding the government, but it sounds like the majority of those standing accused by the National Guard aren't among them.

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.
