Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • January 2016 • 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!

The sky is falling!

Whether you blame global warming, El Niño or the wrath of God, the weather has been pretty freaky lately. From devastating tornadoes in Texas to an unseasonably warm winter on the East Coast, many are feeling cause for concern. Unfortunately, severe weather brings more than heavy rain; it also brings opportunistic scammers looking to prey on those who have fallen victim to destruction, flooding and other by-products of Mother Nature. The Federal Trade Commission (FTC) has issued a warning, stating: "Common natural disaster scams include debris removal and clean-up, shoddy repairs and construction, charity fraud, and imposter scams." The takeaway: If you've been the victim of a natural disaster, don't compound your losses by also falling victim to fraud.

A bad day for payday lenders

Payday lenders, aka loan sharks, are finally starting to pay for their crimes against consumers. The Federal Trade Commission (FTC) just made the largest recovery ever in a payday lending case, collecting over $25 million thus far from a handful of lenders who misrepresented how much their loans would cost consumers. In one instance, the lenders told borrowers that a $300 loan would cost $390 to repay, but ended up charging them $975. Believe it or not, this is pretty standard for a payday loan (the average interest rate is almost 400%!) Payday lenders are getting their due notoriety too, with presidential hopeful Bernie Sanders calling them out in the press, and dozens of politicians and consumer groups (including Consumer Action) demanding more accessible and affordable lending options, such as postal banking, which would allow those who have faced obstacles to opening, maintaining and accessing traditional bank accounts the ability to bank through the United States Postal Service (USPS).

Morally bankrupt

The last thing someone who's filing for bankruptcy needs is to become the victim of a scam, but that's exactly what's happening to many people across the country. We put out a warning about this new (and particularly odious) con last month. Because bankruptcy filings are public records in most areas, nefarious scammers can obtain your personal information (never a good thing) if you've filed. The scam artist then calls you and impersonates a bankruptcy attorney on the telephone through what's known as caller ID "spoofing" (your phone will display the number of an attorney, but the call actually originates from who knows where). Using the information obtained from the public records, the scammer then threatens you with arrest if you don't immediately wire him or her money to satisfy a debt. Hang up! Then pick up the phone and contact your local police department or your state attorney general for help.

'Pharma bro' takedown

So the feds finally took down Martin Shkreli, aka "the most hated man in America," just before the holidays. The wealthy 32-year-old biopharma entrepreneur and hedge fund manager acquired the rights to a lifesaving anti-parasitic drug only to jack the price of each pill up from around $13 to a whopping $750. The moneygrubbing move earned him an unbelievable amount of national notoriety, and the attention of the feds, who concluded that his investment wheelings and dealings at an earlier hedge fund basically amounted to "a Ponzi scheme." According to the indictment, Shkreli now faces two counts of conspiracy to commit securities fraud, two counts of actual securities fraud, and three counts of conspiracy to commit wire fraud due to his reckless mismanagement of investor money. It's hard to feel sorry for the smug "pharma bro," who has issued a series of unrepentant tweets and, as of about a week ago, used his $45 million E-trade account as security for his $5 million bond. The silver lining in the whole mess continues to be hilarious responses like this one from *The New Yorker*, poking fun at what would surely be an outraged response from Shkreli if his lawyer increased attorney's fees the same amount that Shkreli increased drug prices. Talk about irony!

Get-rich-quick scams

Congrats! You've won the lottery! Ah, the tried and true lottery scam—one reader wrote in last month to tell us that she almost fell for one. If someone tells you that you've won big (as long as you pay a fee to collect your winnings), don't buy it. The "fee" nonsense should tip you off every time.

Want to make some cash after the holidays? Emails that promise to pay you if you sign up to be a mystery shopper, a restaurant evaluator or some other retail reviewer are often scams in disguise. While "secret shopping" can bring in extra cash, if you have to pay for a "certification" to apply for assignments or engage in any other sketchy monetary transaction, the gig isn't legit.

Make millions in the stock market! Or not. A lot of otherwise smart people have been duped by "pump and dump" investment fraud (the kind shown in The Wolf of Wall Street movie). The promise of a quick windfall is hard to resist, but if you find yourself tipped off to "the next big thing," think twice before you throw money at it. You could be pumping your hard-earned dollars into a worthless (soon-to-be-dumped) stock that only makes the fraudsters rich. If it were that easy to make money in the stock market, wouldn't everyone be rich?

Tips!

- **Facebook phishing.** This just in: another social media scam, this time directed at those who run a Facebook Page. If you see a popup threatening to disable your page because it has been "reported by other users," don't click! And certainly don't enter your login credentials and credit card information.

- **Dell-lightful.** There's a new tech support scam in town, and it's targeting Dell computer owners. It appears Dell may have suffered a data breach, since the scammers calling and impersonating computer technicians have lots of customer information, including details about prior tech support calls made to the company. Reports have also stated that hackers may have exploited a flaw in an app Dell installed on its computers. You've been warned!

- **A dog-eat-dog world.** Puppy scams aren't cute, but they're increasingly popular as people purchase pets online. Scammers pose as animal breeders, post photos of expensive purebred pets and ask for payment to be sent electronically. Consumers realize they've been duped when Fido never shows up. To avoid this (and be more humane), pick your puppy up from a reputable local breeder or animal rescue agency.

- **Mapping out scams.** The Better Business Bureau's helpful Scam Tracker tool allows you to see what types of scams are happening near you (as reported by fellow consumers). Zoom in to your location on their online map and check it out! You can also upload the details of cons you've encountered and search for scams via keyword (e.g., "credit card" or "rental" scams).

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.
