Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • September 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!

It's raining scams

When the waters rise, scammers come out like sharks smelling blood—and my, how the waters have risen! In the (literal) wake of hurricanes Harvey and Irma, scammers have (drum roll please): helped register over 500 unofficial Harvey-related website domain names to bilk money from donors; sent out countless unsolicited phishing emails with malicious links and booby-trapped attachments; set up fake social media posts tugging at the heartstrings of anyone moved by a seemingly realistic sob story; and even gone so far as to create fake investment pools or bonds, to do everything from "help storm victims" to "contribute to water purification" or "electricity generation." And this is just the start of it: There are also the numerous fake charities and threatening robocalls to victims (often telling them that their insurance premiums are late and they need to pay up or lose out on flood or homeowners insurance). We have to marvel at the scammers' ingenuity though: One created a GoFundMe account pretending to be pop musician Jason Derulo (beware of crowdsourcing scams). Others have benefited from a shortage of construction workers, offering to repair the roofs of desperate homeowners, and even telling them to sign their insurance policies over to hasten the work (don't do it!). Back when Harvey was happening, we wrote a still applicable alert to help consumers recover their losses without losing more to scammers. Check it out, and if you suspect that a scammer has contacted you, report them to the U.S. Dept. of Justice's National Center for Disaster Fraud Hotline via email or phone (866-720-5721) and unleash some fury on *them*. And be sure to keep up to date with the Federal Trade Commission's (FTC) comprehensive "Dealing with Weather Emergencies" webpage, which includes breaking alerts on the latest scams.

The data breach to end (we wish) all breaches

In case you somehow haven't heard, Equifax, one of the three major credit bureaus, has experienced the biggest data breach in the history of data breaches (impacting 143 million people)—which means that if you are a living, breathing being with a credit report, your information has likely been breached. While we

hope that this breach will be the one to *finally* prompt federal regulators to create strong national privacy protections surrounding customer data and requirements that companies notify said customers and take immediate action in the event of a breach, in this newsletter we're focusing on the here and now: What can consumers do immediately to avoid becoming another identity theft casualty? If you've enrolled in Equifax's identity theft protection program, TrustedID Premier (which in itself has been problematic), then you can continue to try to work with the company. Know, however, that Equifax has been flooded with calls and emails from furious consumers, and appears to be in over its head, so it might behoove you to take matters into your own hands. Since the breach actually began three months ago, you should start by checking your credit report(s) immediately for free here. (You're entitled to one free report from each of the bureaus every year, so you could spread this out over time by checking with a different bureau every few months.) If you find that you've fallen prey to identity thieves already, you can begin the process of recovery here. You should also set up a fraud alert so that lenders and credit companies know that you've been a victim of fraud and will take extra caution to verify that "you" are who you say you are. The ultimate step is freezing your credit, which would require anyone requesting credit in your name to provide a PIN that only you've been given. (CNET published a helpful article on what to do and who to contact at each of the credit bureaus to sound the alert or make the big freeze.) Finally, beware of opportunistic scammers calling and pretending to be with Equifax!

Uncle Sam wants you…not to fall for it

Have you heard about the secret bank account at the Federal Reserve that will pay your bills? The one that's been hoarding your cash and just waiting for you to cash in? Does it sound too good to be true? Well, it is. Unfortunately, a sucker is born every minute, which is why the Federal Reserve offered the following all-encompassing warning about the latest scam: "Any video, text, email, phone call, flier or website that describes how to pay bills using a Federal Reserve Bank routing number or using an account at the Federal Reserve Bank is a scam." You see, people don't have bank accounts at the Federal Reserve (that's reserved for banks). And if you try to pay your bills using a nonexistent Federal Reserve account number, it simply won't work, and you could face late fees or worse after your bogus payment is rejected. If you've run across this scam or been contacted by anyone involved in it, you can report it here. (The National Consumer Law Center [NCLC] is collecting these reports and sending them to the FTC. With your help, they may even be able to figure out if/how it benefits scammers to have you attempt to make payments from the Federal Reserve to other parties; right now, it's a bit of a mystery.) The NCLC also says that if you tried to use the bogus payment technique and were charged a returned-payment fee, or ended up paying a late fee because your legitimate payment was then delayed, you could ask the billing company to reverse the fee. Good luck with that, and remember: You should always have *reservations* (get it?) about giving your routing or Social Security number to anyone.

Celebrity scammers?

How the mighty fall. Gwyneth's Goop is finally starting to catch up to her. The celebrity's lifestyle brand website, which hawks mystical, dubiously effective products, has caught the eye of the consumer watchdog Truth in Advertising, which is asking two California district attorneys to investigate 50+ bizarre health-type website claims involving strange products like jade eggs (inserted vaginally) to "prevent uterine prolapse." The group also threatened to sic federal regulators on Goop if it did not remove the bogus claims—a threat that appears to be working.

Et tu, Brady? Famous footballer Tom Brady (he of the good genes) is attempting to profit from his biological blessings, which he chalks up to pseudoscientific wellness products and practices (which, of course, anyone who wants to be like Tom Brady should purchase). Brady claims that strawberries and even coffee (!) have never touched his lips and that his physical prowess is due not to caffeine but to magical PJs and an alkaline diet. Unfortunately, Brady has been working with a known snake oil salesman who has already been penalized by the FTC. If you're gullible enough to buy Brady's BS, you better do it soon, before the FTC gets involved (again).

Playing your cards wrong. Something of a minor celebrity, sports talk personality Craig Carton, who had co-hosted the "Boomer and Carton" radio show alongside NFL quarterback Boomer Esiason for the last decade, was recently arrested for running a massive fake ticket scam, which the *Philadelphia Inquirer* describes as "something out of Mel Brooks' *The Producers*." Let this be a cautionary tale against running up millions in gambling debt (Carton's mistake): Debt will make you do desperate things, particularly if you're looking to, say, avoid a couple of broken kneecaps.

Tips!

- **Infinite indiscretions.** Consumer groups (including us) are calling for more congressional hearings to address Wells Fargo's ongoing bad behavior. It turns out that the bank opened as many as 1.4 million more fraudulent accounts than previously estimated "on behalf of" its unwitting customers. And each day brings fresh news of Wells' wrongdoing: In the last month alone, the bank has been accused of enrolling hundreds of thousands of customer accounts into its online bill pay service (without permission, as is Wells' custom, it seems) and of having charged mortgage applicants unwarranted fees.

- **Deceptive duo.** No, the IRS and FBI have not teamed up to send emails requesting that you click on a link to complete a questionnaire, but scammers sure have. If you click on said link, you download malware that hijacks your computer and demands that you pay up to purge it. (Here are ways to protect yourself against this type of ransomware.) If you've happened upon the email, the IRS says you should file a complaint with the Internet Crime Complaint Center and forward the questionable email to phishing@irs.gov (don't worry, they won't take the bait). And remember: The real IRS will never contact taxpayers by email, text message or social media to request personal or financial information.

- **Out with the old.** Good news! Medicare ID cards, which have historically been vulnerable to identity theft, will no longer display enrollees' Social Security numbers. The Centers for Medicare & Medicaid Services will be getting in touch with recipients soon to replace their out-of-date cards (they are currently figuring out the best way to mail out all the brand spankin' new ones).

- **Against all odds.** No amount of praying, wearing lucky underwear or hand-selecting your own numbers will increase your steadily decreasing chances of winning the Powerball jackpot. As the *Washington Post* points out, playing to win said jackpot may be the biggest scam of all! Since 2015, participants' odds have decreased considerably as the number of balls has increased. According to the *Post*, "Two years ago, your chances of becoming an instant millionaire were 1 in roughly 175 million. Now, the odds are 1 in roughly 292 million."

- **Falling down at the job.** A new study finds big companies woefully vulnerable to phishing attacks. If they would simply adopt technology known as Domain-based Message Authentication, Reporting and

Conformance (DMARC), however, they could dramatically reduce the likelihood that a scammer would be able to impersonate them in an email sent to fool you, the customer. Also according to the study, an unacceptable "92 percent of U.S. Fortune 500 companies have left their customers, partners and brand names vulnerable to domain name spoofing." What can you do? Start by contacting your favorite businesses and asking them to step up their security!

ISO: SWF w/ good credit. In "how does this even happen" news, a woman from Upstate New York was scammed out of a whopping $718,000 on MillionaireMatch.com! After messaging back and forth with an alleged multi-millionaire, the man asked the "highly paid, white-collar professional" to help fund a $7 million business deal. If you think this sounds crazy, the FBI's Internet Crime Center outlines how common it is: Over 14,000 romantics lost more than $219 million in romance scams last year alone. One woman, who fell victim to a man who was ISO women with good credit scores, explained why she used her heart and not her head: "I had just gotten a divorce. I was vulnerable, and he 'wowed' me."

Profiting off empty promises. Manward Press, a pro-"small government/free market" group, is desperately trying to profit off Donald Trump's promise of building infrastructure through the private sector (i.e., selling public roads, bridges and water systems to the highest corporate bidder). Manward's never-ending, scammy-looking website implores "ordinary investors" to throw money at the idea, which they're calling the 1531(b) program. Manward is claiming that "a big chunk of the money [that Trump invests in the infrastructure program] will end up in the pockets of proud U.S. citizens like you and me....Folks who bleed red, white and blue." Manward is, of course, asking these patriots to pay a $49 subscription fee to receive the company's materials, which offer "advice" on how to allegedly claim over $7k in the currently stalled wheelings and dealings.

One ring to bind them. As it turns out, ridiculous deals on bulk items and flat screen TVs aren't the only things you can get at Costco. The mega-wholesaler has also been dealing in knockoff Tiffany rings. While Costco claims that calling the rings in question "Tiffany" was NBD and didn't actually mean customers should take them to be the real deal (apparently, the rings didn't come in the famous little blue box), a court ruled differently. It found Costco guilty of trademark infringement and trademark counterfeiting. So yeah, about that romantic proposal you made to your girlfriend…

Scared straight. A California judge is one of the first to rule that a national "theft diversion" program constitutes extortion. The horrific for-profit program, run by Corrective Education Company (CEC), has also been accused of falsely imprisoning shoppers. Imagine being approached by a security officer as you're perusing the aisle in Burlington Coat Factory, accused of stealing and being strong-armed into watching a video in some sketchy back room. Do it, the security officer says, or he will call the police. The corporate video further outlines your "options": Either "admit guilt" and enroll in a six-hour, $500 "corrective education" course, or go straight to jail (do not pass go, do not collect $200). Unfortunately, even if the recent ruling successfully stops the CEC program from operating in California, it still exists in 25 other states!

Fox, meet hen house. A former dean at disgraced DeVry University, the for-profit school that was charged by the FTC just last year with grossly misleading students about their job prospects upon graduation, is now leading the Department of Education's student aid enforcement unit. This is the unit that is tasked with investigating and punishing sham schools who fail to comply with the law. (We're thinking the new boss—who appears to have no experience in enforcing regulations, by the way—will probably go light on 'em.) Unfortunately, this is yet another example of Education Secretary Betsy DeVos' pro-

corporate, anti-student agenda. Hey, maybe Trump can get back in the game now, too!

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.
