Scam Gram!

Keep the sharks at bay

A Consumer Action News Alert • September 2018 • 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!

#NeverForget

Let's do a checkup: Where are we one year after the largest data breach in history? You know, the one that exposed millions of people's personal and financial information (pretty much everyone in the U.S. with a credit history)? Surely Equifax, the company that was hacked, has been forced to face the music and ultimately adopted better privacy safeguards so that this doesn't happen again, Congress has created meaningful regulations to protect the citizenry, and we—for our part—have done everything we can to plug the burst dam of data that's exploded into the Dark Web and is being sold to crooks around the globe? Er, not quite. "Despite all the outrage and media attention last year, Congress has done little except make security freezes free, and Equifax has not been held accountable," said Chi Chi Wu, staff attorney for the National Consumer Law Center. "And this sensitive information, including Social Security numbers and birth dates, is still out there, with the potential to wreak havoc for the majority of adult American consumers in perpetuity." Perhaps this is why a new NerdWallet survey reveals that 71 percent of Americans report they feel "less secure" over the safety of their financial data and 61 percent still don't feel prepared to handle it when their data is breached. (Also, it doesn't help that a "spousal spy app" has just suffered a data breach.) So what *should* we have learned from the Equifax catastrophe? U.S. PIRG has published a report, *Equifax Breach: 1 Year Later*, on how to protect yourself against ID theft and help hold Equifax accountable. It includes such tips as signing up for a "my Social Security" (MySSA) account (before thieves do) and filing your taxes (before thieves do)—are you seeing a trend here?

Money moves

A number of people have recently reported the peer-to-peer (p2p) mobile payment service Cash App to Consumer Action's Complaint Hotline. The money-exchangers, already frustrated with fraudulent charges,

become even more upset when they Google what they think is a Cash App customer service number only to be re-defrauded by a fake number that scammers have placed in the search results. (As it turns out, the only way to reach Cash App is *through* the app, or via direct message on Twitter.) The debacle brings up two bigger issues, however. First, can you trust p2p payment apps? While these "mobile wallets" (which you allow to connect directly to your bank or credit card account) are great for instantaneously sending a roommate half the rent, the Federal Trade Commission (FTC) recently sued Venmo (one of the largest p2p payment apps) for failing to "disclose material information about the availability of consumers' funds." And Venmo is riddled with privacy problems (in fact, if you're so inclined, you can visit ViceMo to see—in real time—who's using the app to send whom money for sex and drugs, and the various emoji symbols representing them). Cash App, to its credit, doesn't list a public feed of transactions, but when it comes to security and privacy, Consumer Reports says that Cash App and Venmo have nothing on Apple Pay, which it ranks higher in payment authentication and data privacy. (Learn more about safely using p2p payment apps here.) The second issue brought up by the Cash App chaos is that of fake "customer service" numbers and ads listed in online search results. Google (which, like Facebook, doesn't actually list a contact number online) is trying to purge the false info, removing over 100 bad ads per second. But Google can only do so much; the rest is up to you. If you're trying to reach your computer's tech support team or customer service at Cash App, Facebook or any other organization, go directly to its website for the contact info. (Running a Google search for something like "Facebook customer service" will pretty much guarantee bad results.)

Servicemember scandals

(Dot)com cons. The FTC has taken down a number of massive military imposter websites, including fraudulent dot-coms armyenlist and navyenlist. The well-designed sites, which appeared to be officially affiliated with the U.S. military, were actually lead generators that fed the names of those servicemembers and veterans who entered their information to predatory for-profit schools. Representatives from the shady schools would then harangue the prospects, violating "Do Not Call" provisions and posturing as if the secondary schools had the military's endorsement (which is what caught the attention of the FTC). Check out Consumer Action's *Guide to Finding the Right Job Training School* if you're looking for a legit secondary education, and click here if you're looking to join the military. Finally, beware that billionaire Department of Education Secretary Betsy DeVos (put in place by President Trump, of Trump University infamy) couldn't care less about regulating sham schools, so do your due diligence before taking out any student loans.

Benefits boondoggle. On Aug. 18, Comerica Bank put the brakes on its Cardless Benefit Access Service, an ill-fated partnership with the government's Direct Express program that launched in 2017 to allow vulnerable veterans and retirees without bank accounts to access their government benefits through prepaid cards—(here's the clincher) even remotely, without the cards physically present. This ease of use also made it very simple for fraudsters to drain the funds using Direct Express card numbers, PINs and cunning (often phoning the Direct Express call center, claiming to have lost "their" card, in order to have a recipient's payments rerouted). As one disabled marine's caregiver stated, "Direct Express didn't put up a red flag, even though they had all the information about the money being wired to Florida, when we live in Massachusetts, but they just sent the money. We were thinking it was safe because it's [through] the U.S. Treasury." It wasn't, and what's worse is that the now-defunct public-private program, which appears very much to blame due to a complete lack of security protocols/authentication, was *shamefully* slow to stop the fraud when victims implored them to do so. It continues to move at a snail's pace to reimburse lost money, with one victim stating that this all "could have been stopped if Direct Express or Comerica had a fraud unit that could communicate

with customers and law enforcement," adding that "the red tape you have to go through to get to these people [Comerica/Direct Express] is insane. Disabled veterans and the elderly don't stand a chance when their money is taken." Comerica: Clean up your act!

Tips!

- **One of the "good guys."** Sick and twisted scammers are impersonating the very organizations that *warn* consumers of scams in order to make money off those who trust them. The organizations include the National Consumers League, which operates the Fraud.org website; the Better Business Bureau (BBB), which hosts an online scam tracker; and the AARP, which helps vulnerable seniors avoid getting swindled. Impersonators are even taking to Facebook and asking people for money as famous "good guy" Dwayne "The Rock" Johnson. Who's next, Superman? If you're interested in donating to any cause (or person), research official contact information and reach out directly; don't simply respond to a solicitation or offer, even if it appears to come from a well-regarded person or institution.

- **Blending into the crowd.** Crowdfunding cons just keep getting larger and more sophisticated. Case in point: The iBackPack project, which raised over $700,000 in 2015-2016 from backers who have yet to see their Wi-Fi-enabled "smart" satchels (although, oddly, they *have* been shipped accoutrement, like batteries and cables). Then there's this couple, whose home was recently raided by authorities after they withheld the $400,000 they claimed to have raised for a homeless man (who has since sued them for the money). Helpful websites like GoFraudMe can make crowdfunding campaigns a little more transparent, but as Consumer Action's Joe Ridout points out, "At least with a publicly-traded stock, the business is required to provide regular updates to investors about profits, losses, future forecast, etc. Crowdsourcing, by contrast, is completely opaque."

- **In a world of criminals who operate above the law...** You may be so focused on gussying up your ride to make top dollar during a sale that wiping down the dashboard takes precedence over wiping the personal information stored in its electronic systems. This would be a mistake: Unless you're driving an old clunker, your automobile is basically a roaming computer with more digital data on you than KITT had on Michael Knight. Fortunately, the FTC has thought of all the things you might miss in resetting the settings—from garage door codes to "find my car" apps—so head on over to their site *before* you sign your title over to a complete stranger.

- **72: The answer to life, the universe and a phone scam.** If you get a voicemail prompting you to call a number back to find out more, and the message instructs you to dial "*72" before entering the call-back number, don't do it, even if it seems like a dire emergency! Punching in *72 is a little-known way to enact a call forwarding feature that will send all of your future calls to the number that you entered *after* *72 (the scammer's phone), and bill you for the honor. Crooks employ this twisted trick for two reasons: First, they use your number in their international scams (meaning that although you never get the calls from their victims, you *pay* for the calls). Second, they bilk personal or financial info from your friends and family, meaning that when mom thinks she's chatting with you, she's really telling a total stranger to visit more. In other words, hitting *72 could, ultimately, lead to a thief taking your seat at Thanksgiving dinner this year.

- **A tough case to crack.** As summer slides into fall, we find ourselves dreaming of Oktoberfests, craft fairs

and outdoor concerts. Unfortunately, when festival season ramps up, so does rampant fraud. Learn from the unlucky folks in Phoenix who purchased what appeared to be totally legitimate $30-$60 tickets to an all-you-can-eat crab and lobster fest. Arriving with receipts in hand, the crustacean-cravers were met with naught but strip mall. Investigators are still trying to track down the swindlers behind the charade, which was promoted on eTickets(dot)com through a company called "Show Sharks" (how apt) and had been advertised in cities across the U.S. Fortunately, eTickets suspended Show Shark's account, but like the regenerating limb of a lobster, other fake festivals continue to pop up all over the internet. If you're thinking of attending an event, at least make sure there's detailed contact information (e.g., phone numbers) listed on the promoter/event page, and try to buy tickets from trusted sources. The Better Business Bureau has more tips here.

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