The Florida Department of Agriculture and Consumer Services (FDACS) is warning Floridians about unsolicited packages of seeds received through the mail. The seed packets, which may arrive unexpectedly in packages bearing Chinese characters, may bear the name China Post and may be labeled as jewelry, have been reported in multiple states including Virginia, Kansas, Washington, Oklahoma, Louisiana, Utah, and others.

As of July 28, FDACS has received at least 631 reports from Florida residents reporting having received suspicious seed packages. The content of the seed packages remains unknown at this time, until testing by the U.S. Department of Agriculture (USDA) takes place.

The USDA’s Animal and Plant Health Inspection Service (APHIS), the lead regulatory body on this matter, issued guidance. The USDA believes the seeds to be part of a “brushing” scam, where unsolicited items are sent in order to post false customer reviews and boost online sales. Upon receiving seed packages from recipients, the USDA will test the contents to determine if a risk is posed to agriculture or the environment.
The introduction of plant seeds into the United States is tightly regulated by the USDA. Seeds of unknown origin may constitute agricultural smuggling, may be invasive, may introduce pathogens, toxins, or plant and animal diseases, may pose a risk of foodborne illness, and may pose a threat to plant and animal health. FDACS is continuing to work closely to receive additional guidance from the USDA and APHIS, in consultation with U.S. Customs and Border Protection.

“Plant seeds from unknown sources may introduce dangerous pathogens, diseases, or invasive species into Florida, putting agriculture and our state’s plant, animal, and human health at risk,” said Florida Agriculture Commissioner Nikki Fried. “Anyone receiving these suspicious seed packets should not plant them, but should report it to our department immediately, so that our inspectors can safely collect them for analysis.”

**What to Do:** Anyone receiving unsolicited seed packages from other countries should follow these directions:

- **Do not open** the seed packet and avoid opening outer packaging or mailing materials, if possible

- **Place the seed packet AND mailing materials into a sealable plastic bag** – this is important to determining the origin of the seeds

- **Do not plant** the seeds or discard them in trash that will be landfilled

- **Report the seed package** to the FDACS Division of Plant Industry at 1-888-397-1517 or DPIhelpline@FDACS.gov - an Inspector from the FDACS Division of Plant Industry will contact seed recipients to schedule a safe, contactless collection of the seeds, packaging, and mailing materials

When reporting the seed package to FDACS, please be prepared to provide one’s name, physical address, phone number, and email address for contact purposes.
Scammers find new ways to commit fraudulent acts all the time; it seems like it happens daily. Some of their methods are so sinister they are immediately taken as a threat, while others seem a lot less alarming on the surface. One such scam looks a lot less like a potentially harmful crime and a whole lot more like a generous friend or family member, but it could be a sign of trouble. It’s scary because victims may not even know they’re part of something underhanded.

Investigators believe that online sellers – usually overseas – are buying their own products using victims’ names and addresses to appear as independent customers and then leaving a wonderful five-star review for the products. Called a “brushing scam,” box after box of “free” goods show up on victims’ doorsteps, causing them to feel like they just won the lottery instead of being targeted by scammers. One couple found out they were victims of a brushing scam after countless boxes, filled with a seemingly random assortment of items, began arriving at their home.

The victims are not charged for the items in question but also can’t stop the items from being shipped. Scammers engage in this behavior to make the purchase look genuine and avoid violating Amazon’s terms for reviewing one’s own products. Some people might not think of this as being “victims” of a scam. After all, you’re not being charged for the items, no one has touched your credit card (that you know of), and technically, these items aren’t even stolen since the seller is the one who purchased them. Wouldn’t it be neat if some of those boxes contain some new gadgets?

The reality, though, is being involved in a brushing scam means that someone has gained access to your name, mailing address, and potentially other information. What else are they doing with it? Depending on how they accessed your information, they could be privy to a lot more of your personally identifiable information than you realize. Other crimes, such as hacking into a retail website where you legitimately placed an order to get your data, may have led to your information being used in a brushing scam.

If you begin receiving packages that are addressed to you but you did not order, contact the retailer immediately. (Online retailing giant Amazon has stated they will investigate every report of customers receiving unsolicited packages and will ban all vendors and reviewers who abuse the Amazon reviews system.) Then change your passwords on your online accounts, just in case the scammer got your address by hacking an account. If the volume of shipments becomes a problem, as several brushing victims have reported, you can contact the post office for help with holding packages until you can pick them up or otherwise handle the matter.
On July 20, 2020, a federal court in California ruled in favor of the Federal Trade Commission (FTC) in a case against a student loan debt relief firm. The FTC alleged that the operators of Mission Hills Federal, Federal Direct Group, National Secure Processing, and The Student Loan Group bilked borrowers out of millions of dollars. The FTC said the companies lured people with false promises to pay down student loans and lower monthly payments. The FTC also claimed the companies lied about taking over the servicing of the loans, which tricked people into submitting loan payments directly to them. In fact, the defendants diverted borrower payments to themselves.

As a result, the defendants will be permanently banned from the telemarketing and debt relief businesses. What’s more, the ruling also imposes a $27.6 million judgment. The portion of that amount collected by the FTC may be used to refund people affected by the defendants’ scheme. The FTC will provide additional information on possible refunds as that information becomes available.

It’s illegal for companies to charge you for debt relief services before they help you, and some of the companies that promise relief are scams. However, there is help if you or someone you know feels overwhelmed by student loan debt. If you have questions about federal student loans, start with StudentAid.gov/repay. If you have private loans, talk with your loan servicer. For more information, check out ftc.gov/StudentLoans.

In an unrelated debt relief case, the FTC is sending more than $16 million to individuals who lost money to a debt relief scam that targeted tens of thousands of consumers facing financial difficulty. In this case, a group of defendants known as Helping America Group got people to pay hundreds or thousands of dollars a month by falsely promising to pay, settle, or obtain dismissal of their debts and improve their credit scores. Over time, victims found their debts unpaid, their accounts in default, and their credit scores severely damaged—some were sued by their creditors, and some were forced into bankruptcy.

The FTC is providing 27,083 refund checks to victims of the scam. The FTC expects to collect additional money in this case and plans to send a second round of checks at that time.

Recipients should deposit or cash their checks within 90 days. The FTC never requires people to pay money or provide account information to cash a refund check. If recipients have questions about the refunds, they should contact the FTC’s refund administrator, JND Legal Administration, at 833-928-2567.
DECEPTIVE CREDIT CARD INTEREST RATE REDUCTION OFFERS

by Cristina Miranda, Consumer Education Specialist, FTC

Monthly credit card bills can be a drag, especially when you're feeling financially strapped. Finding ways to lower those bills — sometimes by simply calling your credit card company directly and asking for a lower rate — can save you lots of cash. So, what about those companies that call with a “guaranteed” credit card interest rate reduction offer (for a small fee) and a promise to save you thousands of dollars? Most likely, it's a deal designed to dupe you out of money.

According to a complaint by the FTC, three marketers behind the companies CSG Solutions and Second Choice Horizon targeted financially distressed people with illegal robocalls and telemarketing. Their goal, says the FTC, was to sell a bogus credit card interest rate reduction service. For an upfront fee, these companies falsely guaranteed zero percent interest rates for the life of people's credit card debt. They also promised thousands of dollars in savings. But, says the FTC, people never got the financial relief they were looking for.

Instead, the FTC alleges that most people ended up paying extra balance transfer and other fees that they weren't told about, in addition to the companies' hefty fee. The companies also collected Social Security and credit card numbers, security codes, and other personal information over the phone. And, even when the people they called refused to use their service, the marketers used that personal information to apply for credit cards on behalf of those people, without their knowledge or consent. They also sent people invoices, charging them for those cards.

Here's how to protect yourself from this type of scam:

- **The best way to get a lower credit card interest rate is to do it yourself for free.** Call the customer service number on the back of your credit card and ask the company directly for a lower rate.

- **Don't share your credit card, bank account or Social Security numbers, or any other personal information, with telemarketers who call you out of the blue.** Once a scammer has your data, they can use it to commit other fraud against you.

- **It’s illegal for a company to charge a fee before performing a debt relief service, such as reducing your credit card’s interest rate.**

Hang up on unsolicited pre-recorded sales calls. The best way to deal with a robocall is to hang up. You shouldn’t be getting these calls unless you have given the specific company that called you permission to make prerecorded calls to you.
If you're looking for a job, an apartment, or a loan, there's a good chance that someone will be looking at you — closely. They may search for your name online or order a background report. They're looking for red-flag warnings that another candidate may be a safer bet.

According to a lawsuit announced on July 27, 2020, MyLife.com, which sells background reports, raised red flags by posting deceptive “teaser” reports online. The lawsuit says MyLife promoted these reports to employers, landlords, and others to convince them to subscribe to its services. The Department of Justice filed the lawsuit on behalf of the FTC.

Here's how it worked: MyLife displayed the teaser reports when someone typed a person's name into a search bar at MyLife.com. If the person had no criminal, traffic, or sex offender records, the report typically suggested the person had such records. It also prominently displayed large, clickable buttons, one inviting the user to “View [searched-for person’s] Court, Arrest, or Criminal Records,” and another inviting the user to “View [searched-for person’s] Sex Offender Records.” MyLife.com users could view the full records only after paying for a subscription.

In many instances the searched-for people did not have criminal or sexual offender records, or they had minor traffic citations only. As a result, the lawsuit says, the reports were deceptive, violating the FTC Act.

The lawsuit also charges that MyLife didn’t take reasonable steps to make sure its background reports were accurate, violating the Fair Credit Reporting Act, used misleading billing practices, violating the Restore Online Shoppers’ Confidence Act, and didn’t clearly and truthfully disclose that MyLife “had a policy of not making refunds and of discouraging cancellations,” violating the Telemarketing Sales Rule.

Before applying for a job, apartment, or loan, try to fix inaccurate information about you that someone considering your application might see. Start by ordering your free credit reports at AnnualCreditReport.com and disputing any errors you find.
Bitcoin scams come in many different forms. Scammers use different platforms to try and get people to pay them in bitcoin (also known as cryptocurrency or digital money). Bitcoin scams are a popular way for fraudsters to trick people into sending money. Recently, they used Twitter and some of its most notable accounts to target Twitter users.

On July 15, hackers compromised verified Twitter accounts and sent cryptocurrency scam tweets requesting bitcoin donations with the promise of doubling the investments to “give back to the community.” Scammers responsible for bitcoin scams not only aim to steal people’s money, but also collect their personally identifiable information (PII) and sell it to other cybercriminals.

According to Twitter, attackers are believed to have targeted certain Twitter employees through a social engineering scheme. Social engineering schemes use psychological manipulation to trick users into making mistakes or giving away sensitive information. Twitter says the attackers successfully manipulated a small number of employees and used their credentials to access Twitter’s internal systems, including getting through their two-factor protections. This incident proves that even the most technologically-advanced companies are not immune from an employee granting access to bad actors.

Twitter says nearly 130 accounts were targeted, and 45 successfully hacked. The Twitter accounts hacked include high profile individuals with verified accounts such as Barak Obama, Kanye West, Elon Musk, Jeff Bezos, and Bill Gates. Twitter responded by preventing any accounts with the blue verified badge from tweeting while security teams responded to the attack. The blue verified badge on Twitter lets people now that an account of public interest is authentic.

The recent social-engineering hijack of Twitter accounts highlights a larger issue that has been on the increase since COVID-19 began: the prevalence of cryptocurrency scams. According to the Federal Trade Commission, most bitcoin scams appear as emails trying to blackmail someone, online chain-referral schemes, or bogus investment/business opportunities. No matter how the scam is executed, a scammer wants the victim to either send money, give-up their PII, or a combination of both. Once someone sends money, there is usually nothing they can do to get it back.
To avoid a bitcoin scam or other forms of social engineering schemes, remember the following:

- **Never share PII through social media channels and always verify the person or business asking.** While these scams are designed to steal people’s money, they are also designed to collect PII to sell to other cybercriminals.

- **Be cautious of requests for money.** A tweet, email, text message, or other social media post that asks for payment in bitcoin is – most likely – a scam.

- **If an offer seems too good to be true, it probably is.** High profile individuals will not contact anyone to give away large sums of money – especially in bitcoin – by social media message. A “guarantee” to make money is probably a scam.

- **Always be cautious of links that are shared on social media.** No one should ever click a link, download a file, or open an attachment if they are unsure of who sent it or what it is.

- **Keep up with the latest scams and how they work.** The Twitter bitcoin scam employed a lot of common cognitive biases. Understanding how bitcoin or cryptocurrency works reduces the number of people who fall for scams about it.

Visit [www.FloridaConsumerHelp.com](http://www.FloridaConsumerHelp.com) and [www.idtheftcenter.org](http://www.idtheftcenter.org) for more information on scams and fraud.
by Sachit Gali, Intern, 
Division of Consumer & Business Education, FTC

Remember when stores ran out of toilet paper, hand sanitizer, and face masks? Well, now COVID-19 is cause for a new shortage: coins. Because of business shutdowns and social distancing, people have been spending cash at stores or restaurants at record low levels. Adding to the shortage, the U.S. Mint has slowed down coin production for a few months to keep employees safe from COVID-19. Now, some businesses are running low on coins and not offering change.

Here are some tips to avoid losing money next time you go out shopping.

• If you plan on paying in cash when shopping, bring coins from home so you can pay in exact change, if you can.

• If you’re short on change and the store doesn’t have it, ask the cashier if they can offer you store credit or can donate the leftover to charity, which more stores are starting to offer. Or, pay using a credit or debit card — or by check, if accepted by the store.

If a store doesn’t offer change, it should clearly state or display this policy. If you find a store that’s intentionally misleading or deceptive about this policy, call 1-800-HELP-FLA (435-7352) or 1-800-FL-AYUDA (352-9832) for Spanish speakers to report it and obtain information on filing a complaint.

The Florida Department of Agriculture and Consumer Services is the state’s clearinghouse for consumer complaints, protection and information. Consumers who would like information about filing a complaint against a business or who believe fraud has taken place can visit us online at FloridaConsumerHelp.com or contact the department’s consumer protection and information hotline by calling 1-800-HELP-FLA (435-7352) or 1-800-FL-AYUDA (352-9832) for Spanish speakers.