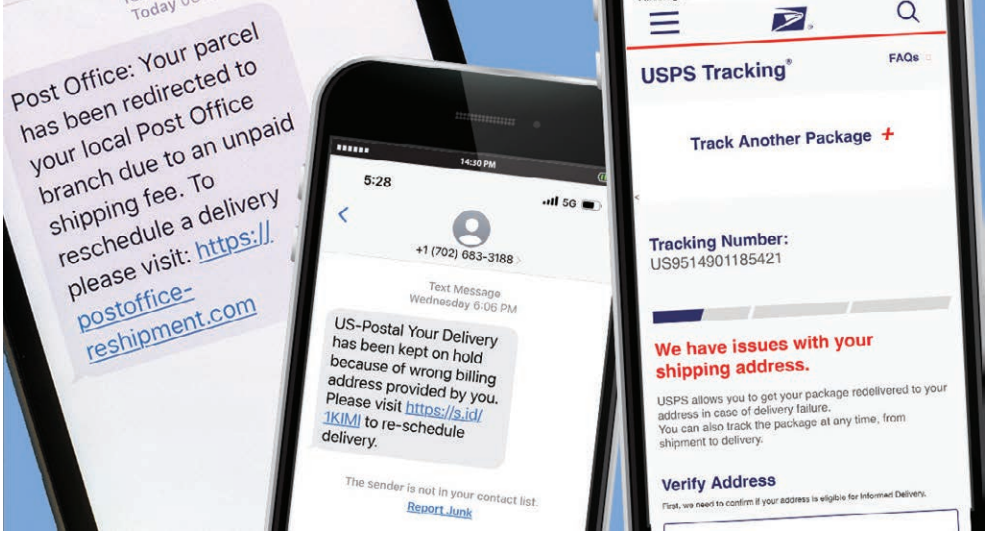


Smishing, brushing and other postal-related scams

Think the internet or smartphones are the only places where all the scammers are trying to take advantage of people today? Think again.

Scammers use the Postal Service to steal by deception in many devious ways, and the payouts can be enormous. Victims have lost their life savings and their homes.

Last year, Patrice Runner, 57, a Canadian man, was sentenced to 10 years in prison for a massive mail fraud scheme uncovered by the U.S. Postal Inspection Service. Postal inspectors say that Runner defrauded 1.3 million victims of a total of at least $175 million before he was caught.

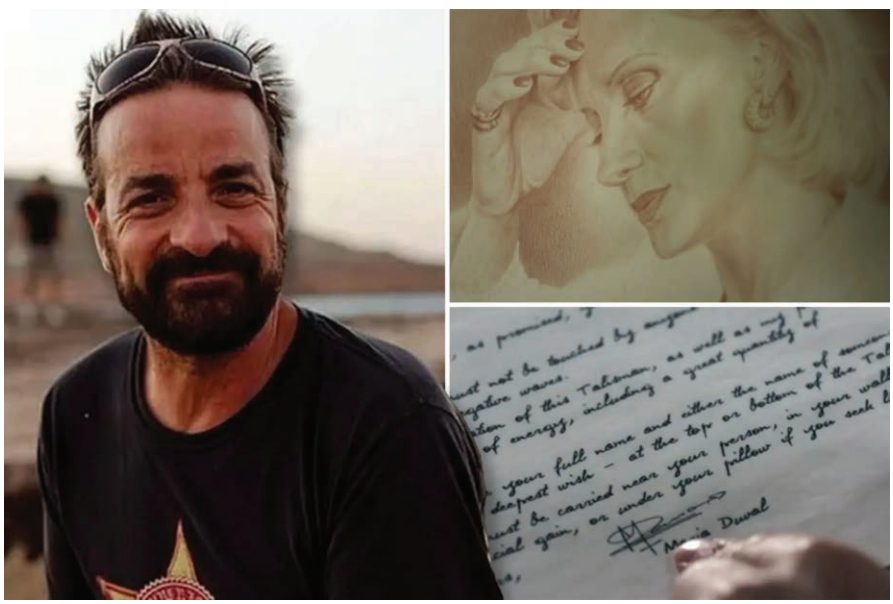
With several co-conspirators, Runner ran a sophisticated mass-mail operation from 1994 to 2014 that sent letters to vulnerable people, often elderly, purportedly sent by a pair of psychics named Maria Duval and Patrick Guerin. In the letters, the psychics promised knowledge that would lead to wealth, better health or happiness—for a fee. Those who sent money back received more and more letters asking for personal information, which was then used to tailor the "psychic" response letters that asked for even more money and information.

Runner's operation was a large-scale international scheme that involved multiple shell companies in several countries to cover up his activities. He used sophisticated mailing machinery, the same kind employed by legitimate mass-mailing companies.

"These letters went out by the tens of millions to every corner of America," Postal Inspector Clayton Gerber said on "Mailin' It," the USPS podcast. "And people paid. They believed it."

Letter carriers can help protect vulnerable postal patrons from scams by keeping a step ahead of the scammers and their latest schemes, as well as by recognizing time-honored fakes and frauds.

Patrice Runner (below) pretended to be a psychic named Maria Duval to bilk victims of their money.



Exploiting trust in the mail

Ironically, scammers who use the mail may gain from distrust of the internet. While many people might recognize an email or text message scam, there's something about a paper

document that feels more reliable, even though it is easy to create fake documents such as checks. Scammers also might capitalize on the trust that Americans have in USPS by using counterfeit Postal Service money orders or other fake USPS documents in their scams.

Perhaps the most well-known scam today is the "Nigerian prince" gambit. The scam always involves asking the victim to put some of their own money in jeopardy in order to pay some kind of bank fee or tax to release a larger payout, which of course never materializes. It's a scam often run through email and social media, but scammers might try to hook victims through the mail by sending counterfeit documents, such as checks or money orders. Sometimes the scammer asks the victim to deposit this check and then keep some of the proceeds and send the rest to a third party immediately. The original check then bounces because it's fake, but the victim has already sent their own money to the scammer.

Nigeria is known as a source of scams, but they can come from all over the world. Scams targeting U.S. Mail customers often originate overseas because it makes it more difficult for U.S. authorities to catch and prosecute the scammers. This was the case with the fraud operation by Runner, who was extradited from Spain for trial.

One prevalent variation of scams run through the mail is a foreign lottery scam. According to scambusters.org, a nonprofit consumer protection group, the scammer tells the victim that they have won a foreign lottery, but that a "remittance fee" must be sent to collect the winnings, or bank account information must be shared.

There are other clever twists to scams that take advantage of the time it takes for a check to bounce and the fraud to be discovered. In one, scammers send a check to the winner first (the check, of course, is fake) with a letter telling the victim it is to cover taxes or fees. The victim is instructed to deposit the check and then transfer their own money to a certain address, which the scammer then intercepts. In another, scammers send victims a check (again, fake) and tell the them they've been chosen as a "mystery shopper." Victims are instructed to buy gift cards with their own funds now and wait for the check to clear, which of course it never does.

In fact, scammers sometimes send official-looking documents impersonating real government agencies to intimidate victims. The documents may warn that the victim owes money for an unpaid speeding ticket or threaten jail time if a fee isn't paid immediately. As with similar scams by email, text or phone call, scammers might demand payment by gift card because gift cards aren't traceable and can't be recovered.

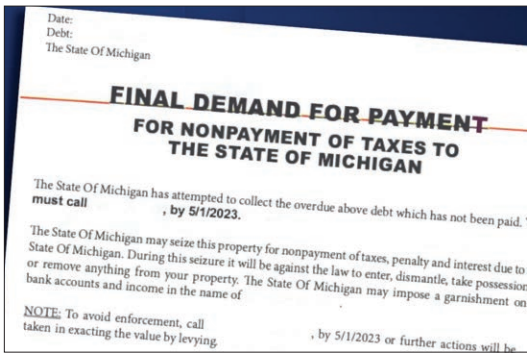
Mail fraud is nothing new

Though the scams keep evolving, scammers have used the mail to defraud people for a long time.

Chain letters have been around at least since 1888, when a missionary school asked supporters to send a dime and then send a copy of the letter to others. Since then, scammers have worked appeals for money or valuables into chain letters. Get-rich-quick offers and Ponzi schemes that ask for investments with guaranteed returns that never come about also have flooded the mail for a long time.

A variation on the get-rich-quick scam promises a way to make money by working from home. Work-from-home scams often prey on people who can't work outside their homes due to disability or caring for children or other loved ones. The scammer simply asks for money for work supplies, often envelopes to stuff for mail marketing, or training materials. Of course, the supplies never arrive.

One of the newest, and perhaps most confusing, postal scams is



Date:
Debt:
The State Of Michigan

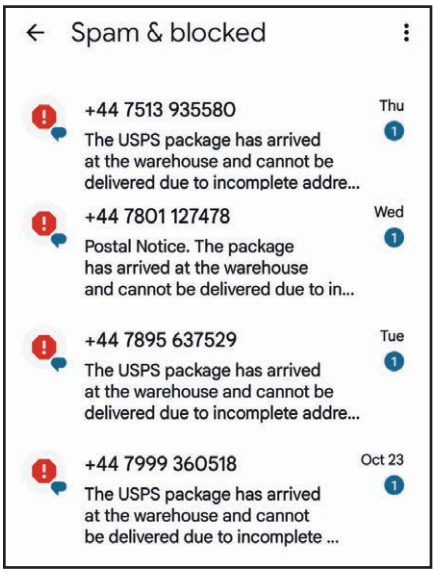
FINAL DEMAND FOR PAYMENT
FOR NONPAYMENT OF TAXES TO THE STATE OF MICHIGAN

The State Of Michigan has attempted to collect the overdue above debt which has not been paid.
must call **, by 5/1/2023.**

The State Of Michigan may seize this property for nonpayment of taxes, penalty and interest due to
State Of Michigan. During this seizure it will be against the law to enter, dismantle, take possession
or remove anything from your property. The State Of Michigan may impose a garnishment on
bank accounts and income in the name of

NOTE: To avoid enforcement, call
taken in exacting the value by levying , by 5/1/2023 or further actions will be

An example of a scam letter that was mailed to residents of Michigan



Examples of smishing

Postal scams (continued)

"brushing." To make an e-commerce listing appear legitimate, an online merchandise seller orders their own product in the victim's name and ships it to the victim's address. The seller then posts a fake positive review using the victim's name. Shipping the item gets around the "verified sale" restriction on reviews, which is designed to screen out fake reviews by people who didn't really buy the item.

While free merchandise may not sound so bad, receiving unsolicited packages can be a sign of a more serious scam—someone may have hacked into the recipients' e-commerce account and ordered merchandise with the intent of stealing it from their porch before they notice or claiming it wasn't delivered to get a refund.

Postal customers may also be victims of "smishing" (SMS phishing) attacks, which happen through email or text but often involve scammers impersonating the Postal Service. The typical smishing message says that delivery of an item was incomplete, and more information is needed to get it to the customer. Inevitably, the scammer asks for something like a credit card number along with a correct address. As with so many scams, the smishing fraud assumes customers who trust the Postal Service will give their personal information before thinking twice.

The romance scam is perhaps one of the most despicable frauds out there. Preying on lonely people, sometimes elderly widows or widowers, romance scammers impersonate a potential mate, showering the victim with love letters that soon ask for money. Once the victim realizes they've been deceived and stops sending money, the fake lover disappears, breaking hearts and emptying bank accounts.

The change-of-address (COA) scam is one that letter carriers are in a good position to spot before customers are victimized. The scammer files a fraudulent change of address for an unknowing postal patron, diverting their mail to the scammer, who either steals financial information from the mail or, if the information was already stolen, hides the bills and statements from the victim. Because they know their customers well, letter carriers often spot suspicious address changes at addresses where the patrons haven't moved away.

Harrisburg, PA Branch 500 member **Christopher Lippy** was honored as the 2022 Special Carrier Alert Hero of the Year for spotting fraudulent COAs and warning his customer (see the June 2023 *Postal Record*).

And, of course, there is plain old mail theft. Thieves may swipe mail from mailboxes or somewhere else in the mail stream and grab personal information to use for identity theft or credit card fraud, or steal checks, cash or packages. Even discarded mail in the trash can be a gold mine for identity thieves, prompting many consumers and businesses to shred their sensitive documents.

"We often talk about the sanctity of the mail, and keeping customers safe from scams can be part of that," NALC President Brian L. Renfroe said. "Protecting the mail from fraud starts with letter carriers. Just as we keep an eye out for people on our routes who need help in an emergency, we should be vigilant about fraud and illegal activity involving the mail."

To report fraud, theft or other crimes involving the mail to postal inspectors, go to uspis.gov/report or call the Postal Inspection Service 24-hour hotline at 877-876-2455. **PR**