The Washington Post
Democracy Dies in Darkness

The stolen-mail scheme now targeting a wealthy D.C. suburb

The theft of checks from USPS blue mailboxes has spiked across the country, and the D.C. region is a new hot spot

By Alisa Tang and Razzan Nakhlawi
April 30, 2022 at 1:48 p.m. EDT

In January, Steve Rosen dropped a check to the Internal Revenue Service in a blue mailbox a block from his home in the affluent D.C. suburb of Chevy Chase, Md. About two weeks later, his bank called him to alert him to fraud. Someone had stolen his check and rewritten it for $13,000.22.

The 59-year-old lawyer immediately filed a report online with the U.S. Postal Inspection Service but says he never heard back from them.

“The real horror was, after it happened the first time, I got a whole new bank account, new checks; a month later, I thought this couldn’t happen again,” he said.

Rosen put the second check — for his tree-care service — into the same U.S. Postal Service mailbox. When he called to ask whether the business had received his payment, it hadn’t. So, he kept an eye on his bank account and again found out that someone had tried to swindle him. That check was repurposed and written out to someone for $2,500.

This time, Rosen didn’t bother with the Postal Inspection Service and instead contacted police in Montgomery County. He was told by the officer taking his report: “Yeah, we’ve had a lot of this going on. You’re not the only one.”

During the coronavirus pandemic, there has been a massive spike in checks being stolen from the mail across the United States and used in financial fraud, authorities and researchers say. In March, the U.S. Postal Inspection Service alerted the Justice Department.

The stolen checks trend is linked to a "significant increase" in armed robberies of USPS letter carriers to steal arrow keys, which can open most mailboxes across an entire Zip code, according to a U.S. Postal Inspection Service advisory to the Justice Department. In some cases, one Zip code can encompass an entire city. The primary motive behind these robberies, the March 7 advisory said, is financial theft: "Criminals are stealing mail … to obtain checks, financial instruments, and personal identifying information to commit bank fraud, mail fraud, wire fraud and identity theft."

Authorities say mail theft has long been a problem, but the use of stolen arrow keys to target USPS mailboxes is new. Law enforcement officials say it's not immediately clear why such thefts have increased.

Georgia State University's Evidence-Based Cybersecurity Research Group has spent the past two years collecting evidence across the Internet of checks stolen from the mail and said this type of crime has spread dramatically over the past three to four months.

Poring over platforms used to sell stolen checks including Telegram, ICQ and WhatsApp, the team of 15 — a professor working with graduate and undergraduate students — first spotted the crime in Florida, California, Texas and New York. Then it started to spread across the country, with the D.C. region recently becoming a new hot spot.

On these platforms, the team spotted about 24 checks from Maryland in October, 98 in December and 431 in January. They've seen a similar trend for D.C.: 12 checks in October, nine in December, then 82 in January. They say that, in the absence of law enforcement and attention to this issue, they expect these numbers to rise.

In a video interview, one of the group's researchers showed The Washington Post several photos of checks stolen from individuals and businesses.

"They have amazing technology," said the researcher, who spoke on the condition of anonymity after receiving threats. "We see some of their labs, and they're well equipped … most of the checks we see come from the blue boxes."

The group found that buyers use nail polish remover to erase the intended payee's name and the amount of the check, replacing the details with their own payee and amount, usually much higher than the original amount. A buyer may also use a fake ID to cash the check at a location such as Walmart.

"Organized crime groups, local gangs are figuring out there's nobody to stop them from doing this," the researcher said.

A Post review of Telegram channels dedicated to check fraud found posts advertising thousands of checks for sale across the United States. The payment amounts ranged from $8 to a business check written out in the amount of more than $36,000, while the checks themselves were on offer to potential buyers for upward of $100, topping out at $400 for business checks.

One Telegram seller offered USPS arrow keys for $5,000 and $7,000 to access mailboxes in Maryland and North Carolina. Another offered a Florida key for $3,000. Several channel administrators said they accepted payment only in bitcoin or Cash App.

The price of the key, the Cybersecurity Research Group said, depends on the area the key is from and how many mailboxes it opens.

The U.S. Postal Inspection Service, responding to an inquiry from The Post, declined to give details about the scope of the problem: "In order to preserve the integrity of our investigations … the U.S. Postal Inspection Service does not confirm, deny, or otherwise comment on the existence of its ongoing investigations."

The Post also asked the Postal Service how it was addressing the problem of stolen arrow keys. “We are continuing to address this issue but unable to provide details for security reasons,” USPS spokesman Dave Partenheimer said.

The Postal Inspection Service offers rewards up to $50,000 for information leading to the arrest and conviction of the suspects who robbed letter carriers. One wanted poster on the Postal Inspection Service website was for suspects involved in robberies that occurred between Nov. 3, 2021, and Jan. 31, 2022, in D.C., Prince George’s County and Montgomery County. It says that postal property, including keys, were stolen.

Montgomery County Police Department Detective Kimberly Ann Pratt says thieves have long targeted residential mailboxes for checks, particularly during the Christmas season. Eight years ago, she said, the trend was for thieves to go early in the morning, look for raised red flags — which indicate there’s outgoing mail in the box — steal the mail and look for checks.

Then in fall of 2020, police saw a shift, Pratt said: “It was no longer stealing checks from residential mailboxes but from big blue USPS mailboxes that sit on the corner. A lot of the mailboxes we saw were not getting pried, were not broken; the assumption was that they were obtaining keys to get into the blue boxes.”

She said from fall of 2020 to now, Montgomery County police have recorded hundreds of reported incidents of mail theft. The areas hit most have been Bethesda, Potomac and Chevy Chase. Though police couldn’t say why these areas are being targeted, they are among the wealthiest suburbs in the D.C. region.

Pratt said sometimes the bank catches the stolen check or the vendor does, if it doesn’t receive a payment. The majority of the time, she said, it’s the customer who notices. She said Montgomery County police are working with postal inspectors on a “large-scale investigation” but declined to give details.

The Postal Inspection Service, the law enforcement arm of the Postal Service, said in an email to The Post that it is working with local, county, state and federal law enforcement to combat mail theft.

It advised customers to hand outgoing mail to their carrier or mail it at the post office; ask their bank for “secure” checks that are more difficult to alter; and report stolen mail by calling 877-876-2455.

The criminal market for checks is thriving, and the blue mailboxes in Steve Rosen’s Zip code — Chevy Chase’s 20815, where census data shows the median home value is $1,012,700 — appear to be compromised. The Cybersecurity Research Group showed The Post a photo it found online of four checks for sale, all from 20815 and dated Feb. 10-12. Two of the victims had no idea their checks had gone missing.

“That’s really shocking,” Susanna F. Fischer, 60, said when informed of her check seen for sale online.

Fischer, a law professor at Catholic University, had put the check for $100 in a blue mailbox near her home as a gift to her niece for her 27th birthday. “She said she didn’t receive it, so I thought maybe I didn’t send it,” she said. “I did not think that it could have been stolen.”

Also in February, Sarah A. Friedman, 48, dropped a check in a blue mailbox to pay a credit card bill. When told about it being for sale on the Internet, she said, “I was going to check on that because I had gotten a late notice, and I knew it was paid on time.”

In Rosen’s case, the two stolen checks were made out to random people, and in both cases the bank restored the money to his account. He says now he doesn’t mail checks, opting instead to pay electronically. He is infuriated that he can no longer rely on the mail.

“It’s a pretty big insult to local citizenry to have s--t stolen from the mail like that. Is that what the Postal Service has come to — that we can’t mail checks anymore? And the answer is ‘yes,’ ” Rosen said.

Meanwhile, the Cybersecurity Research Group researcher — who uses fake “sock puppet” accounts to delve into and research this criminal underworld — also has become a target.

On the day The Post first interviewed the researcher, someone sent him a message on his phone saying they know where he lives, then sent him his Social Security number and address. He spent the next week freezing his credit and putting fraud alerts on all his accounts. He has had police and security surveillance outside his home, paid for by his employer, since then.

Despite these efforts, on April 5 he received by mail a debit card for a Citibank checking account that someone had opened in his name.

Jacob Bogage and Monika Mathur contributed to this report.