How cybercriminals turn paper checks stolen from mailboxes into bitcoin

January 6 2022, by David Maimon


USPS
FOR SALE $3k TOTAL COMES WITH ALL
WORKING ZIPS .

An image of USPS mailbox keys on sale. Screenshot from Telegram

While cybercrime gets a lot of attention from law enforcement and the media these days, I've been documenting a less high-tech threat emerging in recent months: a surge in stolen checks.

Criminals are increasingly targeting U.S. Postal Service and personal mailboxes to pilfer filled-out checks and sell them over the internet using social media platforms. The buyers then alter the payee and amount listed on the checks to rob victims' bank accounts of thousands of dollars. While the banks themselves typically bear the financial burden and reimburse targeted accounts, criminals can use the checks to steal victims' identities, which can have severe consequences.

I founded and now direct Georgia State University's Evidence Based Cybersecurity Research Group, which is aimed at learning what works and what doesn't in preventing cybercrime. For the past two years, we've been surveilling 60 black market communication channels on the internet to learn more about the online fraud ecosystem and gather data on it in a systematic way in order to spot trends.

One thing we didn't expect to see was a surge in purloined checks.

An old threat returns

In general, bank check theft is a type of fraud that involves the stealing and unauthorized cashing of a check.

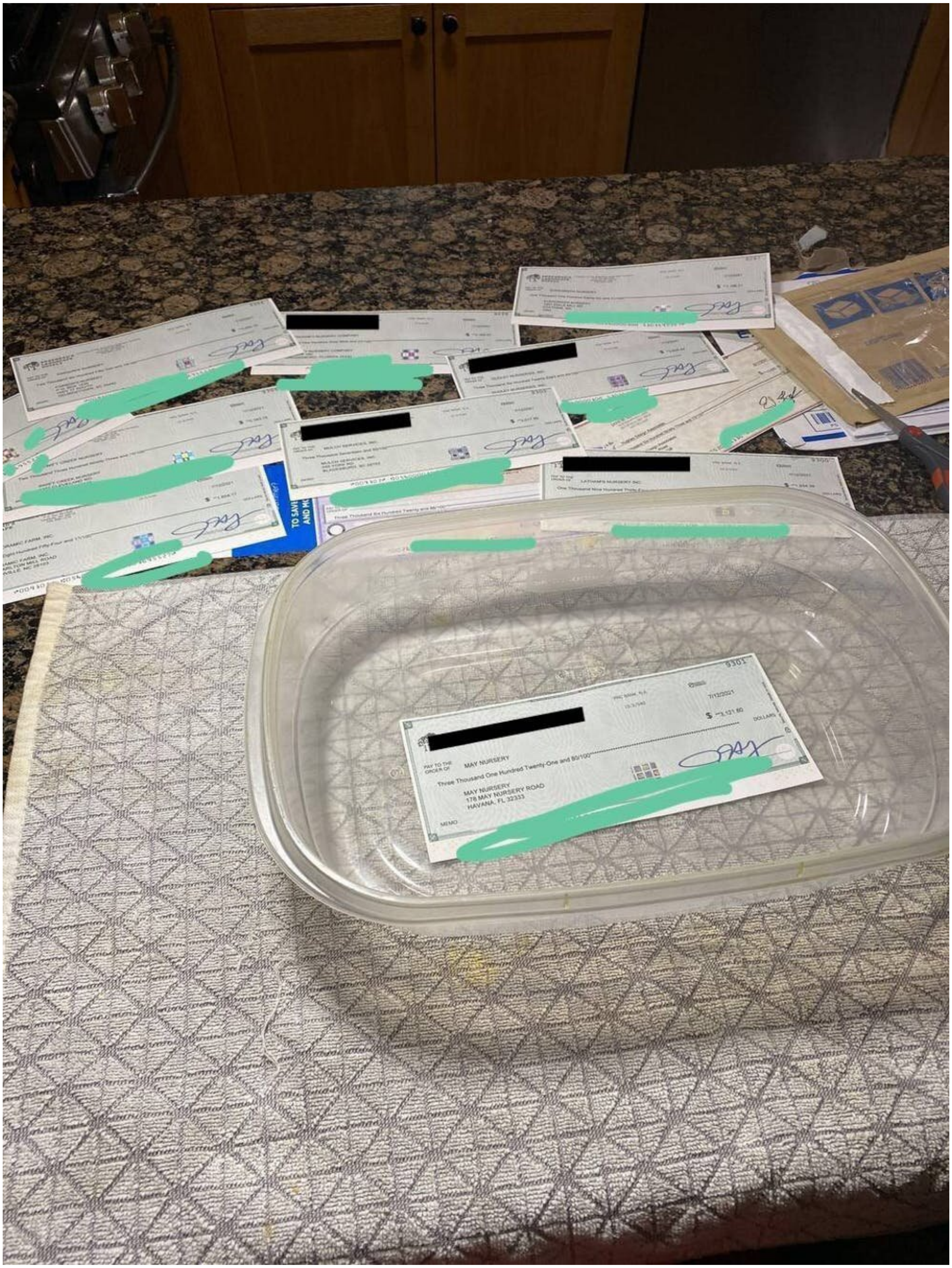
It's hardly a new phenomenon. Criminals were committing check fraud as soon as the first modern checks were cut in the 18th century in England—and the authorities were already looking for ways to prevent it .

While there's little historical data on this type of fraud, we do know it became particularly problematic in the 1990s as the internet made finding willing buyers of illicit items easier than ever. For example, financial institutions estimated they lost about US$1 billion to check fraud from April 1996 to September 1997.

But what may seem a little surprising is that its resurgence now at a time when the vast majority of transactions are conducted electronically and check use continues to wane.

What check fraud looks like

Broadly speaking, the check scams we've been tracking look something like this:


9301
MAY NURSERY
Three Thousand One Hundred Twenty-One and 80/100
MAY NURSERY
178 MAY NURSERY ROAD
HAVANA, FL 32333
MEMO

After stealing a check, criminals use nail polish remover to remove the pen ink used to fill them out. Criminals blacked out the check account and code numbers so they can't be used without purchase. Names and addresses have been blacked out to protect victims' identities. Credit: Screenshot from Telegram

Someone breaks into a mailbox that stores letters waiting to be sent and grabs some of them in hopes they'll contain a check that's been filled in. Often, the crime scene where the theft occurs is the victim's own mailbox, but it can also be one of those blue USPS boxes you pass on the street.

Criminals can access those with a stolen or copied mailbox key, which we have seen on sale for as much as $1,000.

Thieves may deposit or cash the checks themselves or sell them on to others via a marketplace of illicit items, such as fake IDs and credit cards. Prices are typically $175 for personal checks and $250 for business ones—payable in bitcoin—but always negotiable and cheaper in bulk, based on our observations and direct interactions with the sellers.

Buyers then use nail polish remover to erase the intended payee's name and the amount displayed on the check, replacing those details with their own preferred payee—such as a retailer—and amount, usually a lot higher than the original check. A buyer might also simply cash the check at a location like Walmart using a fake ID.

In some cases we believe criminals are using the checks to steal the victim's identity by using their name and address to manufacture fake driver's licenses, passports and other legal documents. Upon taking over someone's identity, a criminal may use it to submit false applications for loans and credit cards, access the victim's bank accounts and engage in

other types of online fraud.

Tracking black market chat rooms

To better understand how cybercriminals operate, my team of graduate students began monitoring 60 online chat room channels where we knew people were trafficking in fraudulent documents. Examples of these types of channels are group chats on messaging apps like WhatsApp, ICQ and Telegram, in which users post pictures of items they wish to sell. Some of the channels we are monitoring are public, while others required an invitation, which we managed to procure.

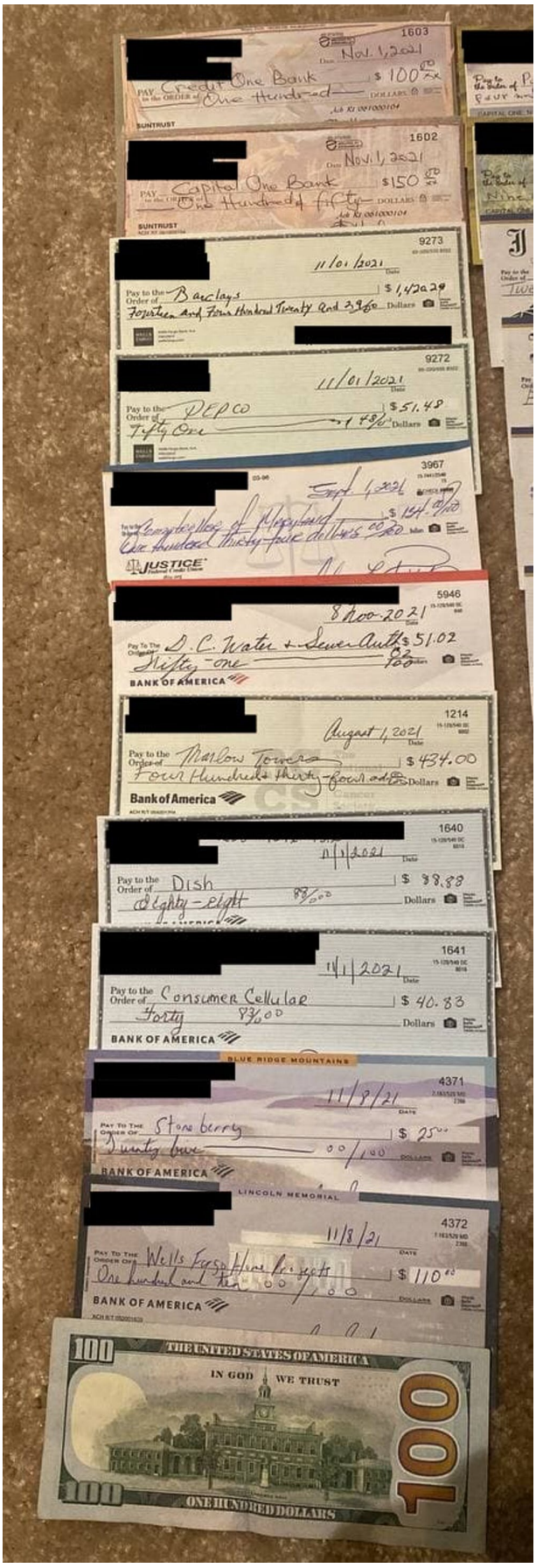
After we noticed a rise in stolen checks on sale, we began systematically gathering data from those channels about six months ago in order to track the trend. We downloaded the images, coded them and then aggregated the data so we could spot trends in what was being sold.

In our observations, we came across an average of 1,325 stolen checks being sold every week in October 2021, up from 634 per week in September and 409 in August. Although little historical data on this practice exists, a one-week pilot study we conducted in October 2020 places these numbers in some perspective. Back then, we observed only 158 stolen checks during that period.

Furthermore, these figures likely only represent a small fraction of the number of checks actually being stolen and sold. We focused on only 60 markets, when in fact there are thousands currently active.

In dollar amounts, we found that the face value of the checks, as written, was $11.6 million in all of October and $10.2 million in September. But again, these values likely represent a small share of the actual amount of money being stolen from victims because criminals often rewrite the checks for much higher amounts.

Using the victims addresses, which appeared on the left top corner of the checks, and focusing on the data we collected in the month of October 2021, we found New York, Florida, Texas and California were the top sources.


1603
Nov. 1, 2021
Pay to the Order of Credit One Bank
$ 100
One Hundred
SUNTRUST
1602
Nov. 1, 2021
Pay to the Order of Capital One Bank
$ 150
One Hundred fifty
SUNTRUST
9273
11/01/2021
Pay to the Order of Barclays
$ 1,420.29
Fourteen And Four Hundred Twenty And 29/100 Dollars
9272
11/01/2021
Pay to the Order of PEPCO
$ 51.48
Fifty One
3967
Sept. 1, 2021
$ 134.00
JUSTICE
5946
8-00-2021
Pay To The Order Of D.C. Water + Sewer Auth
$ 51.02
Fifty-one
BANK OF AMERICA
1214
August 1, 2021
Pay to the Order of Marlow Towers
$ 434.00
Four Hundred thirty-four and 00/100 Dollars
Bank of America
1640
11/1/2021
Pay to the Order of Dish
$ 38.88
Eighty-eight
1641
11/1/2021
Pay to the Order of Consumer Cellular
$ 40.83
Forty
BANK OF AMERICA
BLUE RIDGE MOUNTAINS
4371
11/8/21
Pay To The Order Of Stone berry
$ 25.00
Twenty five
BANK OF AMERICA
LINCOLN MEMORIAL
4372
11/8/21
Pay To The Order Of Wells Fargo Home Mortgage
$ 110.00
One hundred and ten
BANK OF AMERICA
100
THE UNITED STATES OF AMERICA
IN GOD WE TRUST
100
ONE HUNDRED DOLLARS

Stolen personal checks typically go for $175 – but they're cheaper purchased in bulk. Credit: Screenshot from ICQ

How to protect yourself

The best advice I can give consumers who want to avoid falling victim to these schemes is to avoid mailing checks, if you can.

Bank checking accounts usually offer customers the option to send money electronically, whether to a friend or a company, for free. And there are many apps and other services that allow you to make digital payments from bank accounts or via credit card. While there are risks with these methods as well, in general they are a lot safer than writing a check and sending it in the mail.

Still, some types of businesses may require a physical check for payment, such as landlords, utilities and insurance companies. Moreover, as a matter of personal preference, some people—myself included—prefer to pay their bills using checks rather than other methods of payment.

To avoid the risk, I make sure to drop off all my letters containing checks inside my local post office. That's generally your best bet for keeping them out of the hands of criminals and ensuring they reach their intended destination.

The United States Postal Inspection Service, the agency responsible for preventing mail theft, also offers tips to stay protected.

As for enforcement, the inspection service works with the police and others to crack down on mail-related crime. These efforts result in the arrest of thousands of mail and packages thieves every year. However, for every arrest, there are many more criminals who go undetected.

And when we informed officials of our findings, they were also surprised by what we discovered but planned to step up monitoring of these types of black market communication channels.

Our research suggests much more systematic data on this type of fraud is needed in order to better understand how it works, crack down on the activity and prevent it from occurring in the first place.

Provided by The Conversation