The New York Times https://www.nytimes.com/2024/07/29/business/retirement-savings-scams.html

SWINDLED SAVINGS

How One Man Lost $740,000 to Scammers Targeting His Retirement Savings

Criminals on the internet are increasingly going after Americans over the age of 60 because they are viewed as having the largest piles of savings.

Listen to this article · 11:15 min Learn more

By Tara Siegel Bernard
Tara Siegel Bernard spoke to people who've fallen victim to scams that target savings of Americans, particularly older adults. This article is the first in a series.

July 29, 2024

For nearly three months, Barry Heitin, a 76-year-old retired lawyer, thought he was part of a government investigation that felt like something out of the movies. He was actually assisting criminals in stealing hundreds of thousands of dollars — of his own money.

Last fall, he spent just about every weekday doing the legwork and making withdrawals from his bank accounts as part of an intricate scam: He believed he was helping the feds safeguard his money and catch thieves who were after it.

"They kept telling me, 'This is a big case and we are going to stop a whole ring of people,'" Mr. Heitin said. "It was like a rabbit hole. I was going down the hole with them."

It cost him almost all of his retirement savings: roughly $740,000.

Americans spend a lot of energy saving for retirement and worrying about losing money to the gyrations of the stock market. But these days, sophisticated criminals — on dating sites, on social media, in messaging apps or using malicious software — present an ever-growing risk to people and their savings.

The nature of these schemes makes it nearly impossible to recover the money, leaving victims with little recourse. The stolen funds are often whisked to overseas accounts or laundered through cryptocurrency wallets, which are quickly emptied.

Mr. Heitin was one of many people interviewed by The New York Times who were ensnared in scams that could be so elaborate it's as if they were created in a writer's room testing different plot devices. Scammers can impersonate government officials, tech support staff or love interests. They coach victims on how to sidestep fraud prevention measures at financial institutions, and they use manipulative psychological tactics — isolation, a sense of urgency or preying on people's willingness to trust or connect — to keep the scam going.

"The crime doesn't end until they have taken all of your money," said Erin West, a prosecutor with the district attorney's office in Santa Clara, Calif., who leads a cybercrime task force. "It is going to hit every victim the same exact way until they lose everything they have, whether it is $5,000 or $50,000 or $15 million."

Compounding the pain, there can even be a hefty tax bill waiting for them after they've drained their retirement accounts.

Potential losses from cybercrime exceeded $12.5 billion in 2023, a 22 percent jump from 2022, and more than triple the levels in 2019, according to the F.B.I.'s Internet Crime Complaint Center. But these figures underestimate the problem, since many victims don't report their losses.

People over 60, often targeted by cybercriminals because they are viewed as having the largest piles of savings, experienced the steepest losses among all age groups in 2023, at more than $3.4 billion, according to the F.B.I.

The receipts and documentation from Mr. Heitin's scam. Hailey Sadler for The New York Times

The computer and phone Mr. Heitin had been using when he fell victim to the scam. He kept them, but no longer uses them. Hailey Sadler for The New York Times

Ensnared in a Fake Investigation

For Mr. Heitin, it began in September, when he was unable to log into his 401(k) retirement account. When he tried again several days later, he got in, but the screen quickly changed and instructed him to call the 401(k) provider's fraud department. He called the number on the screen, which had the firm's logo on it.

That's when he connected with a man who called himself Charles Hunt and said he was a fraud investigation officer with the firm. (Mr. Heitin and his lawyer said they didn't want to name the institutions because they were in discussions about

possible restitution.)

Mr. Hunt told Mr. Heitin that someone was trying to gain access to his account.

Then, he named a big bank where Mr. Heitin held an I.R.A., as well as checking and savings accounts. That money was vulnerable, too, he was told. Mr. Hunt then connected him with a man who called himself Hayden Smith, who said he was with the bank where Mr. Heitin kept his checking account.

Mr. Smith said he had identified two $10,000 transactions for purchases of child sexual abuse imagery through a site in China. He peppered Mr. Heitin with questions. “Ever been to China? Know anyone in China? Buy anything in China?”

He had not. Next, Mr. Heitin was told that financial institutions often worked with the federal government on these cases. Would he be willing to talk with them?

That’s when a third man, who identified himself as Finn Whitrock, came on the line and said he was with the Internal Revenue Service. He provided a badge number and said that Mr. Heitin’s other accounts were at risk, but that the government could safeguard his money by transferring it to a federal locker.

If he was willing to cooperate with their investigation, Mr. Whitrock explained, Mr. Heitin could play a critical role in preventing a ring of criminals from preying on others — while ensuring he wouldn’t lose the $20,000 the thieves had tried to steal. But they needed to move quickly.

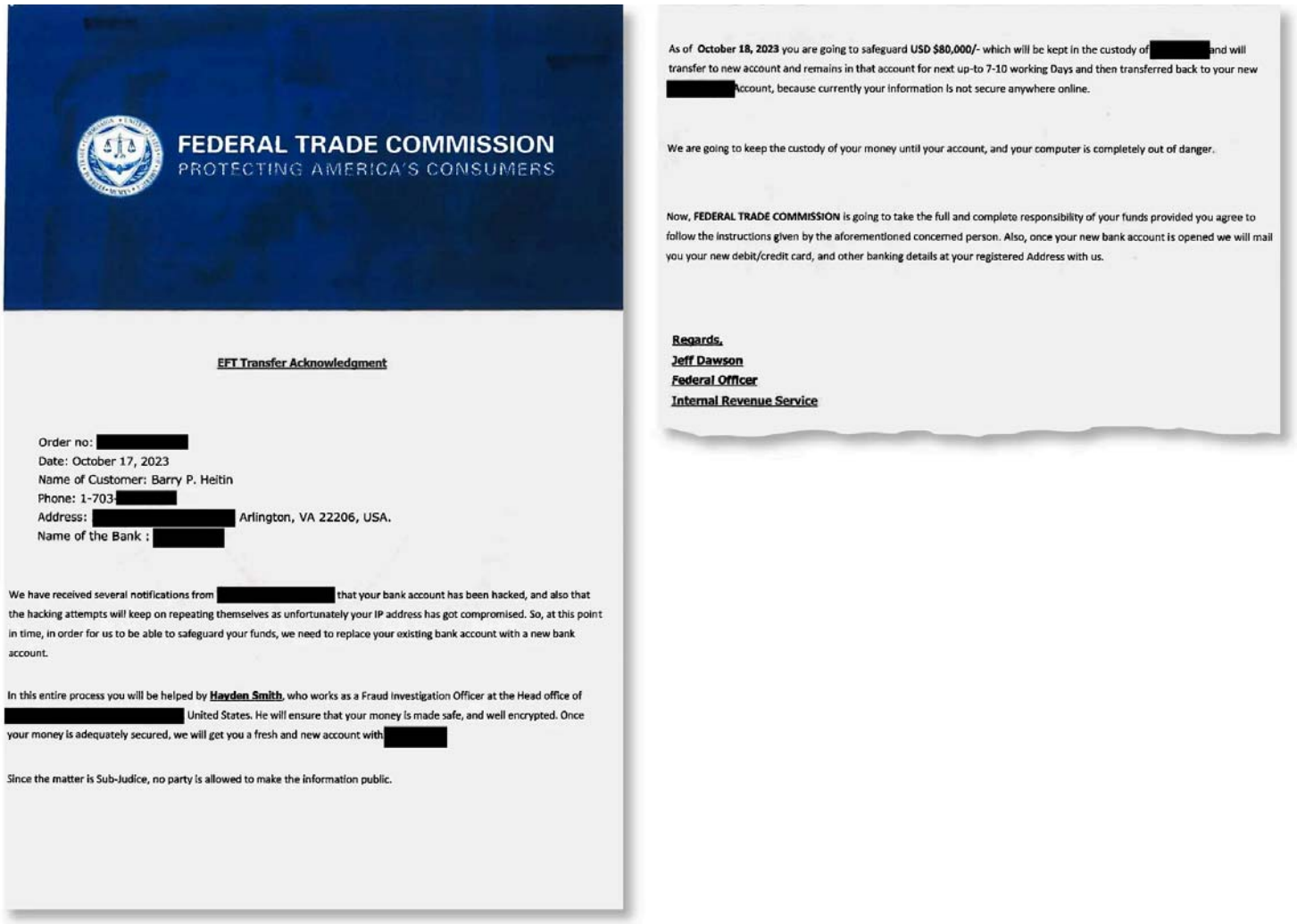
“Let’s do it,” Mr. Heitin said he had told them. “I then gave them access to my computer, and they started me in a series of withdrawals from my banks accounts.”

He began withdrawing his retirement money and other savings, transferring them to what he believed was a secure place, largely using Bitcoin, A.T.M.s and wire transfers to other accounts.

Mr. Heitin, who lives alone, was instructed not to disclose anything to anyone, including his three adult children.

The impostors kept close tabs on him. Mr. Smith walked him through all the transactions, so they spoke daily. Mr. Hunt called him every morning and evening; they developed a friendly rapport, swapping stories about cars and bad knees.

Throughout the ordeal, Mr. Heitin's computer was running around the clock — the criminals had loaded an image of a world map onto his machine with flashing lines sprouting in different directions. Mr. Hunt would refer to that map, and give him periodic updates on the fictitious thieves. Interpol had snagged at least one of them. Another had been tracked to Singapore.



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

EFT Transfer Acknowledgment

Order no: [redacted]
Date: October 17, 2023
Name of Customer: Barry P. Heitin
Phone: 1-703-[redacted]
Address: [redacted] Arlington, VA 22206, USA.
Name of the Bank : [redacted]

We have received several notifications from [redacted] that your bank account has been hacked, and also that the hacking attempts will keep on repeating themselves as unfortunately your IP address has got compromised. So, at this point in time, in order for us to be able to safeguard your funds, we need to replace your existing bank account with a new bank account.

In this entire process you will be helped by **Hayden Smith**, who works as a Fraud Investigation Officer at the Head office of [redacted] United States. He will ensure that your money is made safe, and well encrypted. Once your money is adequately secured, we will get you a fresh and new account with [redacted]

Since the matter is Sub-Judice, no party is allowed to make the information public.

As of **October 18, 2023** you are going to safeguard **USD $80,000/-** which will be kept in the custody of [redacted] and will transfer to new account and remains in that account for next up-to 7-10 working Days and then transferred back to your new [redacted] Account, because currently your information is not secure anywhere online.

We are going to keep the custody of your money until your account, and your computer is completely out of danger.

Now, **FEDERAL TRADE COMMISSION** is going to take the full and complete responsibility of your funds provided you agree to follow the instructions given by the aforementioned concerned person. Also, once your new bank account is opened we will mail you your new debit/credit card, and other banking details at your registered Address with us.

Regards,
Jeff Dawson
Federal Officer
Internal Revenue Service

The letter, sent to Mr. Heitin, looks official at first glance, but provides some clues. It was printed on Federal Trade Commission letterhead, for example, but was signed by a federal officer from the Internal Revenue Service. The New York Times

Draining His Retirement

After Mr. Heitin pulled out a total of $113,000 from his checking and savings accounts, he was instructed to move his retirement money to accounts where he could more easily transact.

Those transfers would be trickier: He had more than $830,000 in his I.R.A. and brokerage account, and his adviser of more than 20 years would have questions.

But the scammers had a ready-made excuse. Mr. Heitin would explain that he was buying a property in Canada and produce a listing to show the bank. “It was a surprise for my kids,” he was coached to say.

His adviser didn’t buy it. The bank made some calls — the property hadn’t been sold, it told him. There hadn’t even been any inquiries.

So, using Mr. Smith’s suggestion, Mr. Heitin said he needed the money to buy gold. That’s when the bank asked him to come in.

Before he went, his handlers began planting seeds of doubt, leading Mr. Heitin to believe that his personal information might have been leaked through the branch. Mr. Whitrock — the man who claimed to be from the I.R.S. — rattled off a list of five names, asking if he knew any.

Mr. Heitin knew the last one: It was his adviser. He hadn’t been accused of anything yet, Mr. Whitrock said, but he was on a watch list.

“That put me on the defensive,” Mr. Heitin recalled.

At the bank, he pressed his adviser, the branch manager and a compliance person to just give him his money, but he left empty-handed.

Mr. Heitin kept his receipts and documentation in an expanding folder. Hailey Sadler for The New York Times

Mr. Smith came up with another idea: Roll the I.R.A. over to a different institution. That worked.

Mr. Heitin now had $834,000 in the new I.R.A., which he emptied in under two weeks, with no questions asked by the new provider, and moved the money into bank accounts.

“This type of activity is a classic sign of potential money-laundering activity and should have raised red flags,” said Robert Rabinowitz, Mr. Heitin’s lawyer, who is trying to help Mr. Heitin recover some of the funds.

Investment firms are required to “make a reasonable effort” to obtain a trusted contact when accounts are opened or updated — someone who can be alerted should firms have reason to believe a customer is being exploited. Firms are also

permitted — but not required — to temporarily freeze transactions or disbursements.

In Mr. Heitin's case, the institution that suspected something was amiss didn't have a contact on file, but when it tried to establish one, he was already deeply embroiled in the scam.

Once the money was easily accessible, Mr. Heitin was on a mission to get it to safety.

Some days, he would bounce between two bank branches, withdrawing $5,000 from each. When the banks started asking questions, he was instructed to wire money to a gold dealer in New York, who also tried to warn him.

"I'm concerned for you," Mr. Heitin recalled the dealer saying as he told him about another customer who was lured into buying gold for a scammer.

Mr. Heitin ultimately made three purchases — totaling roughly $416,000 — of gold ingots and coins.

Within hours of each purchase, they were out of his hands. With Mr. Smith in his ear, he'd wait for a car to drive up to his apartment building and deposit the gold, in a brown paper bag, into the back seat.

"It seemed very James Bond-ish," he said. "I was trying to get to an end point."

Mr. Heitin realized he had become a victim of a scam after being contacted by a detective who had found his name on a receipt for a gold purchase. Hailey Sadler for The New York Times

The Scheme Unravels

That point came in late November, when he received a call from a detective in New Jersey. She had found his name and address on a paper receipt for gold in a car.

“I’m pretty sure you’re the victim of a scam,” he recalled her saying. “I almost had a let down, or a sense of relief,” he said. “I felt good and bad at the same time. It is hard to explain.”

Eventually, he met with two F.B.I. agents at his daughter’s house, and later learned he was among at least seven other victims pulled into a scheme based in India.

“My dad was set up for a very comfortable retirement and he is just not anymore,” said Liana Loewus, Mr. Heitin’s daughter. “One of the most difficult parts of the aftermath of a scam like this is that it feels like no one cares.”

Her father’s ordeal isn’t over.

Withdrawals from tax-advantaged retirement accounts like traditional I.R.A.s are taxed as ordinary income, so to the government, it looks like Mr. Heitin lived large last year: He still owes nearly $285,000 in federal and state taxes.

There used to be relief for victims of personal casualties, disasters and theft in the form of a tax deduction, but that was eliminated as part of the Republican-led overhaul of the tax code in 2018.

A bill that was introduced this year would reinstate the deduction, and Mr. Heitin’s lawyer said he planned to seek an individual tax ruling from the I.R.S.

Today, Mr. Heitin’s tainted laptop sits at the bottom of his kitchen pantry, out of sight. But he still thinks about his ordeal all the time.

“Do I look back on it and say I probably should have done other things?” Mr. Heitin said. “Of course. But I have to get past that. If I don’t, I’m stuck in a horrible depressive loop. With the help of my family and the support of those around me, I am past that.”

Tara Siegel Bernard writes about personal finance, from saving for college to paying for retirement and everything in between. More about Tara Siegel Bernard