

Bilked and Bereft

Surging cyber scams leave older Vermonters destitute, frustrated and saddled with tax debt

BY DEREK BROUWER • derek@sevendaysvt.com

JANA SLEEMAN



The scam that cost Jeanette Voss her life savings began with alarm bells.

In 2021, the 67-year-old Bennington woman opened her laptop to watch Netflix. A siren-like screech blared from the speakers, and a message appeared: Her computer had been hacked, and Voss needed to contact Microsoft for help.

Voss called the phone number that appeared on her screen. The man who answered was able to silence the shrieking. Then he explained to Voss that hackers had already obtained her Social Security number. To protect her financial accounts, Voss would need to transfer her funds into what he called a secure digital wallet until the U.S. government could issue her a new Social Security number. He and another man could walk Voss through the process, but they had to work discreetly; the hacker's identity was unknown.

“Trust no one,” Voss recalled the man saying, “for your safety.”

For the next six months, Voss talked to the two men almost every day, using a prepaid cellphone that they told her to buy because hers had been compromised. She dubbed the burner device her “batphone.” During each call, Voss would scribble their detailed instructions across three spiral notebooks.

And, as instructed, she would painstakingly move her savings — retirement funds, stocks, certificates of deposit — into the bank accounts and cryptocurrency wallets they had provided.

Then the men vanished. So did her money, all \$950,000 of it.

Cyber scams have flourished since the pandemic as transnational crime rings leverage cryptocurrency and artificial intelligence to advance their increasingly sophisticated, ever-shifting schemes. Older adults such as Voss are prime targets, experts say, because they may have nest eggs to plunder, are perceived as less tech savvy and are more likely to be isolated. Americans who are 60 and older lost nearly \$3.5 billion to scams last year, according to reports filed with the Federal Bureau of Investigation's

cybercrime center, up from less than \$1 billion in 2020.

More than 150 older Vermonters told the FBI that they'd been scammed last year for a collective \$4.8 million. The true tally is almost certainly much higher. Cyber scams often go unreported by victims who feel shame or humiliation. As Vermont continues to grow older, more residents will enter the target zone.

The crimes can devastate victims, and not just financially. Many confront hopelessness and feel that they've been stripped of their dignity. Some spiral into pits of depression. Perpetrators, often overseas, rarely face justice.

Little help is available in Vermont to seniors such as Voss. They are largely on their own to manage a financial catastrophe while navigating bureaucratic mazes.

During and following her scam, Voss became malnourished and addicted to painkillers that she had been prescribed for her multiple sclerosis. More than three years later, she still hasn't told her son or other family members about what

happened, even though she missed a relative's funeral because she could no longer afford the trip. She has learned to survive solely on her \$2,065 monthly Social Security checks, unplugging her electronic appliances when not using them to save a few dollars each month.

Victims who drain their retirement funds as part of a scam are still typically liable for federal and state taxes on those withdrawals. So a massive tax bill further complicated her situation.

Voss, now 70, described living with "unrelenting stress" for more than three years. "From that moment of the screaming coming out of my computer," she said, "until, well ... It's just ongoing."

'THIS MUST BE REAL'

The man who answered Voss' call introduced himself as a Microsoft employee named Thomas Anderson. His South Asian accent seemed not to match the European-sounding name, but Voss was willing to hear him out. She had spent much of her career working in marketing and human resources for Intuit, maker of TurboTax tax

Voss was becoming ensnared in a particularly insidious version of one of the most common cyber ruses: the tech-support scam.

preparation software, so she understood that American tech companies outsource customer support to places such as India.

"Anderson" claimed that a gambling website had received a whopping \$231,500 bet from Voss' bank account. When she denied placing the wager, Anderson told her that he wanted to run a diagnostic scan of her laptop to assess the breach. He instructed Voss to download free software that would enable him to access her computer remotely.

Voss watched along as lines of code raced across her screen. The name of the

investment advisory firm that managed her retirement accounts appeared.

Oh, this must be real, she thought.

Voss was becoming ensnared in a particularly insidious version of one of the most common cyber ruses: the tech-support scam. By impersonating trusted companies, scammers convince victims that their computer or phone has been compromised, then offer to help. Sometimes they steal a few hundred dollars for fictitious antivirus software and move on. But if they can hook a victim who has a pot of savings, scammers will methodically extract everything they can get.

The schemes tend to target seniors, who account for more than half of the \$924 million stolen through tech-support scams last year, according to the FBI. The Vermont Attorney General's Office receives more reports about tech-support scams than any other type of cyber fraud, Attorney General Charity Clark said.

The screeching sound and pop-up message that scared Voss had likely been lying in wait on her laptop for some time, according to Doug Shadel, a nationally recognized fraud expert who previously worked for AARP. Bits of code that trigger the pop-ups typically make their way onto victims' computers through web surfing. Clicking on something as innocuous as an ad on Facebook can quietly trigger the download of malware that serves as scam bait.

"A week or a month later, this pop-up occurs with a phone number to call and sirens going off," Shadel said. "You call the number because you're panicked."

From there, impersonators mix together the three ingredients that Shadel said make any scam work. They endeavor to build trust, put the victim into a heightened emotional state and create a sense of urgency to act.

Voss would not strike most as an easy mark. She is smart, comfortable using computers and a little quirky, with tortoiseshell glasses that sit askew on her round nose. She raised her son on her own in Southern California before saving enough to retire at age 59 and move to Vermont.

Research that Shadel helped conduct for AARP suggests personality traits aren't necessarily what make someone

BILKED AND BEREFT » P.28



SCAM ALERT!

Cyber thieves are getting more creative, but you can learn to recognize suspect pitches.

SOME RED FLAGS



- Somebody asks you not to tell anyone else about their communication.
- Being asked for your Social Security number, Medicare number or bank information.
- Does the situation sound incredible? Listen to your own doubt.
- Beware requests to wire money or pay with cash, cryptocurrency or gift cards. (The safest way to make payments: credit cards.)
- Somebody requests remote access to your computer.

TYPICAL SCRIPTS

Tech support — An urgent message warns a computer is compromised.



Imposter — A scammer claims to represent a government agency or business.

Romance — A scammer gains trust via a romantic relationship online.

Grandparent — A caller claims a grandchild is in serious trouble.

WHAT DO EXPERTS ADVISE?

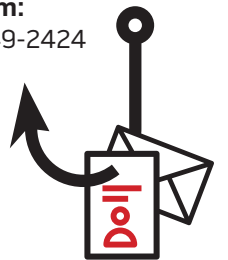
- You don't have to answer an unexpected phone call or message. Scammers can "spoof" real phone numbers to make themselves appear legitimate.
- Feeling unsure? Hang up.
- Received a scary pop-up? Turn off your computer.
- Talk about scam safety with friends or family. Identify a trusted contact to consult before sending money or giving someone access to your computer. You can also add a trusted contact to your financial accounts.



FOR MORE ADVICE

AARP Fraud Watch Network Helpline has volunteers trained to help spot fraud: 877-908-3360 or aarp.org/fraudwatchnetwork

Vermont Attorney General's Office Consumer Assistance Program: 800-649-2424



WERE YOU SCAMMED? REPORT IT ASAP TO:

Vermont Attorney General's Consumer Assistance Program: 800-649-2424

AARP Fraud Watch Network Helpline: 877-908-3360

U.S. Department of Justice National Elder Fraud Hotline: 833-FRAUD-11

FBI cyber crime center: ic3.gov

Local police

FIND SUPPORT

AARP hosts online support groups for victims of cyber fraud: aarp.org/fraudsupport

Vermont Legal Aid can help with tax issues: 800-889-2047, vtlawhelp.org/taxes

Tip sheet adapted from AARP, Vermont Attorney General's Office and Vermont Department of Financial Regulation



Bilked and Bereft « P.27

susceptible to a scam. AARP surveys found that victims were more likely to have experienced recent stressful events.

“Maybe it’s less about *who* you are,” Shadel said, “and more about *how* you are at the moment of the encounter.”

The months before that pop-up appeared on Voss’ screen on Memorial Day 2021 were a particularly difficult period in her life. The previous November, her son was attacked in San Diego and blinded in one eye. A few months later, her brother drove off the road in the same city, hitting and killing three homeless people who were sheltering on the sidewalk. He faced criminal charges.

Voss had been processing those shocks from her quiet home in Bennington, where she has lived alone since 2018. She had resided in Bennington once before, during her twenties, and upon retirement decided to return to the place where she remembered feeling happiest in her life. She bought a single-story home at the end of a dead-end street. Voss, who has an offbeat sense of humor, installed a tombstone at the bottom of the driveway with the epitaph, “The end of the road.”

After Anderson gained access to Voss’ laptop, he told her he was going to connect her with a member of the fraud team at the financial advisory firm whose name had flashed across her screen. That second man, he explained, would help Voss move her assets into a secure cryptocurrency account until her identity was protected.

During the first phone call, Voss filled a page in her notebook with passwords she would need to change, IP addresses and other guidance from Anderson. At the bottom corner of the page, she jotted a “secure” phone number for this second contact and drew a box around it for emphasis. Below that, she noted his alias: “Alan Maxwell.”

‘YOU’RE THE VICTIM’

Over the weeks and months that followed, “Maxwell” coached Voss on the logistics of liquidating her financial portfolio. She moved her funds first into checking accounts, then wired the money to various cryptocurrency wallets.

Between June and September, Voss completed at least 15 wire transfers, according to a spreadsheet she kept. Each time, she visited her local bank. Tellers were sometimes skeptical and asked probing questions about the transactions. But Maxwell had prepared Voss with false stories about her reasons for



Attorney General Charity Clark at AARP Vermont's Scam Jam at Bugbee Senior Center in White River Junction



Guests at AARP Vermont's Scam Jam



Jeanette Voss consulting her fraud documentation

transferring so much money. He also told Voss to bring her batphone to the bank so he could listen to the conversations.

After her bank, Bank of Bennington, refused to authorize any more wire transfers, Maxwell directed Voss to open an account at People's United Bank as a workaround. When People's refused to process the transfers, she moved her money to Citizens Bank in August and sent several more.

Voss told no one about the ordeal, even as it consumed her daily life. The scammers specifically told her not to contact her professional financial adviser — who, Voss later learned, had noticed the withdrawals she was making but did not ask her about them at the time.

Voss was living in a state of constant fear. She was racing against time, worried the supposed hacker would access her accounts before she was able to move all her money. She stewed over who had stolen her identity: Was it someone she knew and trusted, as

Anderson and Maxwell seemed to suggest? Voss asked Google to blur the image of her home on the company's maps service, grasping for any scrap of privacy.

Voss also grappled with creeping doubts about those two men. At one point, she confronted them about their implausible names. They always had an answer.

Voss called Maxwell on her batphone one night around 9 p.m. to confide how anxious she felt. He reassured her that "it will be over soon," according to her notes from the call. She apologized for bothering him so late.

"Talked me off ledge," she scribbled after another call with Maxwell.

Voss didn't know much about cryptocurrency, just that it was supposedly the next big thing. To scammers, mainstream acceptance of digital money has been a major boon. Transactions are irreversible and difficult to trace, even on established exchanges. Nearly half of all cyber-scam

losses reported to the FBI by older adults last year involved cryptocurrency — a sevenfold increase since 2021, when Voss was scammed.

Over the past 18 months, the Vermont Attorney General's Office has received five reports of cyber thefts with losses exceeding \$500,000. Four of them involved cryptocurrency; one tech-support scam victim reported losing \$3 million.

Vermont lawmakers earlier this year passed a bill to limit how much money can be deposited at ATM-like crypto-

Federal prosecutors in the Western District of Pennsylvania brought indictments against three men involved in Voss' scam.

Thien Phuc Tran, 33, was accused of laundering the money Voss had deposited into cryptocurrency accounts from his residence in Santa Ana, Calif. His brother-in-law — 30-year-old Ton Huynh Bui — and 34-year-old Tien Nguyen, of Sachse, Texas, were accused of helping Tran carry out the scheme. They weren't Anderson and Maxwell — those still-unidentified men worked with Tran, Bui

Maybe it's less about *who* you are and more about *how* you are at the moment of the encounter.

DOUG SHADEL

currency kiosks, which have become popular tools for scammers. The law also bans installation of new kiosks for one year.

But the scammers are resourceful. Earlier this year, an 87-year-old Wolcott woman caught in a tech-support scam was told to travel to a Bitcoin kiosk in Littleton, N.H., to deposit her cash into a digital wallet.

She wasn't able to use the machine, so the scammers hatched another plan, said Lamoille County Sheriff's Department Det. Sgt. Kevin Lehoe, who helped investigate the case. Back home, the woman placed \$20,000 cash inside a cardboard box and taped it shut. A Massachusetts woman named Rachel Chen drove to her rural home to retrieve the money, prosecutors in New Hampshire allege in an ongoing case. Chen has since been accused of working as a courier, or mule, for a cyber-scam ring, Assistant Attorney General Bryan J. Townsend II said.

Voss moved nearly all of her money into cryptocurrency wallets — except for \$10,000, which Maxwell said she could keep in cash. She waited for a new Social Security card to arrive by mail, as Maxwell and Anderson promised.

The card never came. The men stopped responding.

"FUCKED!" Voss wrote in her notebook.

She called her financial adviser and the Social Security Administration. She went to the Bennington Police Department and filed a report with Officer Amanda Knox.

Later, an FBI agent came to Voss' house, took another statement and reviewed her documents.

Then something unusual happened.

and Nguyen out of an illicit call center in India, prosecutors allege.

The prospect of recovering any of Voss' money remained slim. But the criminal investigation brought some clarity while she was feeling profoundly disoriented. As she walked out of the Bennington Police Department the day she filed her initial police report, Voss asked the officer a question: "Officer Knox, am I going to be arrested?"

"Jeanette," she said Knox replied, "you're the victim."

TURBO TAXED

The scammers had left Voss with just \$10,000. But by cashing out her investments and retirement accounts, she also had incurred an enormous tax bill. In the eyes of the Internal Revenue Service, her taxable income in 2021 was \$635,300, which put her in the top 1 percent of Vermont earners. That meant Voss owed \$134,000 to the federal government and \$41,000 to the state.

Voss couldn't afford to hire a tax specialist to fight back, but the AARP fraud hotline pointed her to the sole tax attorney at Vermont Legal Aid, Zachary Lees.

Lees explained to Voss that she could try to cut deals with state and federal authorities to lower her bill. But the process would be long and laborious, with no guarantees. Lees planned to show that Voss had no ability to pay such huge amounts while also arguing that reducing the bills was the fair thing to do.

To make the case, Voss needed to assemble a mountain of records to prove

Bilked and Bereft

« P.29

the fraud was real and that it had left her broke. The process is burdensome for anyone, Lees said, and beyond what some older taxpayers can handle.

“It is so friggin’ onerous for them to have to fill out these forms, to go to the bank and pull bank account statements,” he said.

Voss was overwhelmed. At the same time, she was cooperating with an FBI investigation, signing up for heating assistance and food stamps to afford groceries, and trying to manage her runaway emotions. Each month, a new letter from the Vermont Department of Taxes arrived to remind her of the penalties and interest accruing on her bill.

“I was freaking out on so many levels,” Voss said.

At Lees’ suggestion, she separated stacks of paperwork into different rooms of her house to help herself focus on one problem at a time.

Scam victims did not always face this additional financial burden. For decades, the federal tax code included a deduction for theft losses.

In 2017, congressional Republicans went searching for revenue to offset other tax cuts. They pared down the deduction as part of the Tax Cuts and Jobs Act of 2017 championed by former president Donald Trump. That provision, like many in the bill, will expire at the end of next year. In the meantime, elderly scam victims have been ordered to pay hundreds of thousands of dollars to the IRS after being robbed of their life savings, according to a *Washington Post* investigation and an April report by Democrats on the Senate Special Committee on Aging.

Martha “Mickey” Pullen, a 79-year-old Strafford woman, owes more than \$63,000 in state and federal taxes after falling victim to a cyber scam in 2020. She drained her \$200,000 retirement account during the monthslong con. Pullen told *Seven Days* that the subsequent tax bills make her “furious.”

“I feel totally betrayed by the government,” Pullen said.

U.S. Sen. Peter Welch (D-Vt.) cosponsored legislation in March that would reinstate the deduction and provide retroactive tax relief for victims, but Congress has taken no action on it. He introduced the bill after hearing complaints from scam victims in Vermont.

“It’s outrageous,” Welch said in a statement at the time.

After months of preparation, Voss and Lees submitted her tax requests in July 2023. By early this year, Vermont agreed

to reduce Voss’ tax bill to just \$25. Voss agreed separately to pay \$1,000 to the IRS.

But she had another issue to resolve: her property taxes. Voss’ high taxable income in 2021 instantly made her ineligible for the state credits that help low-income seniors afford their property taxes. Voss asked the Bennington Board of Abatement to reduce her bill from \$6,400 to the \$1,350 she would have owed with the credit in place.

Voss appeared before the board at its annual meeting last December. Board members listened, then deliberated in closed session. The next day, Voss received their written decision. Board members expressed sympathy for her situation, but they claimed their hands were tied by state law. The board denied Voss’ request for relief.

She paid the bill.

‘IT JUST SHOULDN’T BE THIS HARD’

In Strafford, Pullen, a retired nurse, has had a harder time coping.

Like Voss, Pullen fell victim to a pernicious scam that began with a pop-up on her MacBook Air urging her to call “Apple Tech Support.” For weeks, she talked daily with several men — one, “John Watson,” claimed to work for the Social Security Administration — as they directed her to empty her retirement account.

The scam unfolded between November and December 2020, during the COVID-19 pandemic, when Pullen was more isolated than at any point in her life. She lived alone with almost no visitors, stepping out only for occasional, masked trips for groceries. She read a book a day.

Losing her entire retirement savings plunged Pullen into despair. She had hoped to pass the money as inheritance to her daughter, Emma Bullock, who is raising two children in Montréal. Convinced she had stolen her daughter’s future, Pullen felt stupid, helpless and bitter. She began talking about suicide.

When a volunteer helped Pullen prepare her tax return the following spring, Pullen was shocked by the \$63,000 bill and decided not to file at all.

“I just naïvely thought, *Well, it’ll go away*,” Pullen said. “They don’t go after Trump — why should they go after me?”

After a couple of years, the tax agencies came knocking. In April, the State of Vermont secured a lien on the two-bedroom home where Pullen has lived since 2015, her only major asset.

COURTESY OF SHEILA KEATING



Martha “Mickey” Pullen

I feel totally betrayed by the government.

MARTHA “MICKEY” PULLEN

Negative thoughts consumed her. Pullen was admitted within the past year to the psychiatric care ward at Dartmouth-Hitchcock Medical Center, where she had worked for 25 years as a nurse in a surgical special-care unit. Her physical health declined as well; she is losing her hearing and sight in one eye.

Her daughter said it has been difficult to watch Pullen flounder.

“I feel like I’ve not only lost all that money,” Bullock said, “but I’ve also lost my mother.”

Sheila Keating, a part-time community nurse hired last year by the Town of Strafford, has been helping Pullen

the best she can. Along with a neighbor, Keating organized a sale of Pullen’s quilting supplies to supplement her roughly \$1,600 monthly Social Security checks. Keating has offered emotional support and companionship.

She and the daughter are also trying to help Pullen gather documents so she can seek the same sort of tax relief that Voss obtained in Bennington. They have been working for months with Lees, of Legal Aid, but still aren’t ready to file her petitions with the tax authorities.

“It’s an absolute disaster,” Keating said. “It just shouldn’t be this hard.”

State officials work to prevent scams through education and awareness. The Attorney General Office’s Consumer Assistance Program takes scam reports and occasionally helps recover money for victims who immediately report the theft. The office also issues alerts about the latest scams, and Attorney General Clark speaks at public seminars.

Victims can call an AARP fraud hotline for advice. But the state does not provide anything close to specialized case management for victims of

catastrophic losses — which is exactly what Pullen needs, Keating said.

What's available today "is not good enough," she said. "It just isn't — not for the elderly population."

Vermont has a nonprofit Financial Abuse Specialist Team, but the organization has no money beyond small grants that fund an annual conference, founder Victoria Lloyd said. Lloyd, a former Vermont Adult Protective Services investigator, said the state needs an office dedicated to supporting victims of fraud, abuse and financial exploitation.

"We're not providing a safety net for them," she said.

Last week, Attorney General Clark addressed 30 or so seniors at an AARP Vermont fraud seminar in White River Junction. Most attendees said they had been targeted by cyber scams, and more than a few raised their hands when asked if they had lost money to one.

After the event, Clark said victims would benefit from more intensive support. When she and her staff hear of severe scam situations, they sometimes think, *These people need a caseworker*, Clark said.

It's not a service she said her office can afford to provide. The money would need to come from the state legislature or the federal government, Clark said.

On a recent August afternoon, Keating sat with Pullen at her dining table. Dozens of family photos were displayed on a side table behind them. Pullen looked sharp in a crisp button-down shirt and freshly washed hair; Keating had persuaded her fellow nurse to spruce herself up for a reporter's visit.

"I rely on Sheila to keep me on the straight and narrow," Pullen explained. "I was going to commit suicide. I still may, but it won't be until it's all settled."

Keating interjected: "But I keep reminding her how much she means to me. So, she can't do that."

'AN ABSOLUTE NIGHTMARE'

In Bennington, Voss found support in peer therapy groups that she had been attending before the 2021 scam. After she told a couple of friends from the groups what had happened, one offered to mow her lawn because Voss could no longer afford to hire someone to do it. The other friend donated a tractor to make the mowing easier.

She has learned to get by on her Social Security income and gained back the 25 pounds she lost during the peak of her distress. She weaned herself off her multiple sclerosis medication, to which she had become addicted. Her files about the scam stay tucked away in

a closet where she doesn't have to look at them. She plans eventually to destroy the papers in a bonfire.

"I'm healthy now, and I'm exercising," Voss said. "I can say honestly that I am content with my life the way it is at the moment. It could get better, but I am content."

The FBI investigation uncovered some details about the perpetrators who scammed her. Tran and Bui, the brothers-in-law from California, and Nguyen, of Texas, worked with others,

wallets using information stolen from victims and to quickly launder the money that victims transferred into them. Tran and others used the funds to buy prepaid debit cards, pay credit card bills and make mortgage payments. Some of the money was sent to Vietnam and India, prosecutors said.

Tran, Bui and Nguyen admitted last fall to conspiring to launder money.

Voss' contacts, Maxwell and Anderson, may have been low-level players in the sprawling transnational enterprise.

with dementia symptoms to her bank to transfer funds. Nicholas Melanson, 42, had been recruited into the scam through a woman he "met" online. The woman, whom Melanson never saw in person, duped him into believing she shared his romantic interest. The arrangement was a kind of "scam on top of a scam," said Nikolas Kerest, U.S. Attorney for the District of Vermont.

Prosecutors typically try to unravel organized crime rings by prosecuting low-level participants such as Melanson or Chen — the courier in Wolcott — then working up the chain of command. But Melanson didn't even know who he was working for.

"Their scams are sophisticated, and their efforts to keep themselves insulated are sophisticated as well," Kerest said.

That's one reason the convictions of Tran, Bui and Nguyen in the Western District of Pennsylvania were notable. Federal prosecutors mentioned the difficulty of catching higher-level operatives in asking a judge to sentence them to prison time.

"It is important that every participant in the conspiracy receive just punishment to serve as a deterrent to others," the feds told the court.

Bui and Nguyen were each ordered to serve four months in prison, which they did earlier this year. Federal prosecutors sought a longer term for Tran, who they said laundered most of the stolen funds.

In January, U.S. District Court Judge J. Nicholas Ranjan sentenced Tran to seven years and three months in prison — the maximum term under federal guidelines.

Voss submitted a statement in advance of the hearing. Preparing it was painful, she wrote, but she wanted others to understand how the crime affected her life.

"The situation has been an absolute nightmare for me," she wrote. "Imagine for yourself what you would do if this crime were to happen to you or a loved one."

In issuing the sentence, the judge ordered Tran, a legal permanent resident who was out on bond, to surrender himself to a federal prison in Louisiana by March 11.

Tran never showed up.

After *Seven Days* discovered that Tran was on the lam, Voss contacted her victim assistance specialist with the U.S. Department of Justice for more information. For months, Voss had assumed that Tran was in prison.

"Tran is unfortunately a fugitive," the advocate replied earlier this month. "We believe he likely left the country on a fraudulent passport." ⑦



Photo of Thien Phuc Tran and his family from his federal court file

including an illicit call center in India, to steal at least \$4.2 million from more than 20 people. At the same time the man who called himself Maxwell was coaching Voss, he was bilking an 83-year-old Pennsylvania man out of nearly \$1.3 million, investigators discovered.

Prosecutors described Tran as a "leader" of a scheme that spanned California, India and Vietnam. Tran recruited Bui, Nguyen and others to set up bank accounts and cryptocurrency

Many who work in illicit call centers in places such as India are young people who struggle to find legitimate employment, a *New York Times* report found. Some scammers in other countries are coerced into the work by criminal syndicates with threats and false promises, the *Times* recently reported.

Last month, federal prosecutors in Vermont secured a six-month prison sentence for a New Hampshire man who escorted an elderly Windsor woman